GUTRIDE SAFIER LLP
Seth A. Safier (State Bar No. 197427)
seth@gutridesafier.com
Marie A. McCrary (State Bar No. 262670)
marie@gutridesafier.com
Todd Kennedy (State Bar No. 250267)
todd@gutridesafier.com
Kali R. Backer (State Bar No. 342492)
kali@gutridesafier.com
100 Pine Street, Suite 1250
San Francisco, CA 94111
Telephone: (415) 639-9090
Facsimile: (415) 449-6469

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MARCO WALSH, HOWARD YOSHA, and ERICA MALDONADO, as individuals, on behalf of themselves, the general public, and those similarly situated,

Plaintiffs,

v.

DOLLAR TREE STORES, INC.,

Defendant.

CASE NO.

CLASS ACTION COMPLAINT FOR INVASION OF PRIVACY; INTRUSION UPON SECLUSION; WIRETAPPING IN VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (CALIFORNIA PENAL CODE § 631); USE OF A PEN REGISTER IN VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (CALIFORNIA PENAL CODE § 638.51); COMMON LAW FRAUD, DECEIT AND/OR MISREPRESENTATION; UNJUST ENRICHMENT; BREACH OF CONTRACT; BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING; AND TRESPASS TO CHATTELS

JURY TRIAL DEMANDED

TABLE OF CONTENTS

INTRODUCTION 4

THE PARTIES....6

JURISDICTION AND VENUE 6

SUBSTANTIVE ALLEGATIONS 7

A. Defendant Programmed the Websites to Include Third-Party Resources that Utilize Cookie Trackers. 7

B. Defendant Falsely Informed Users That They Could Reject the Websites' Use of Advertising Cookies....12

C. Defendant's Conduct Violated Its Own Privacy Policy. 17

D. The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting Defendant's Websites....17

1. Google Cookies....17

2. Facebook Cookies....23

3. Microsoft Bing Cookies....25

4. Additional Third Party Cookies 27

E. The Private Communications Collected are Valuable. 29

PLAINTIFFS' EXPERIENCES 30

CLASS ALLEGATIONS 38

CAUSES OF ACTION....40

First Cause of Action: Invasion of Privacy....40

Second Cause of Action: Intrusion Upon Seclusion....43

Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy Act (California Penal Code § 631)....44

Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of Privacy Act (California Penal Code § 638.51) 49

Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation....51

Sixth Cause of Action: Unjust Enrichment....53

Seventh Cause of Action: Breach of Contract 54

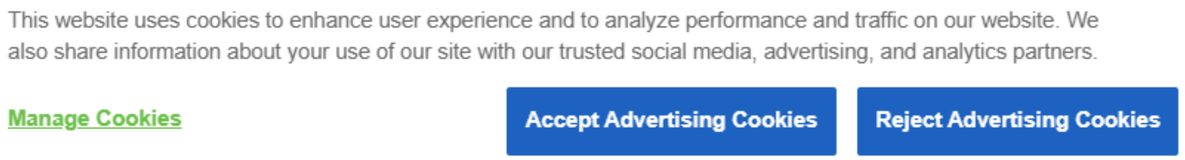
Eighth Cause of Action: Breach of Implied Covenant of Good Faith and Fair Dealing ...56

Ninth Cause of Action: Trespass to Chattels 57

Plaintiffs Marco Walsh, Howard Yosha, and Erica Maldonado ("Plaintiffs") bring this action on behalf of themselves, the general public, and all others similarly situated against Dollar Tree Stores, Inc. ("Defendant" or "Dollar Tree"). Plaintiffs' allegations against Defendant are based upon information and belief and upon investigation of Plaintiffs' counsel, except for allegations specifically pertaining to Plaintiffs, which are based upon Plaintiffs' personal knowledge.

INTRODUCTION

1. This Class Action Complaint concerns an egregious privacy violation and total breach of consumer trust in violation of California law. When consumers visit Defendant's ecommerce websites (www.dollartree.com and www.familydollar.com, each a "Website" and collectively, the "Websites"), Defendant displays to them a popup cookie consent banner. Defendant's cookie banner discloses that the Websites use cookies but expressly gives users the option to control how they are tracked and how their personal data is used. Defendant assures visitors that they can choose to "Reject Advertising Cookies" as shown in the following screenshot:



This website uses cookies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our trusted social media, advertising, and analytics partners.

2. Like most internet websites, Defendant designed the Websites to include resources and programming scripts from third parties that enable those parties to place cookies and other similar tracking technologies on visitors' browsers and devices and/or transmit cookies along with user data. However, unlike other websites, Defendant's Websites offers consumers a choice to browse without being tracked, followed, and targeted by third party data brokers and advertisers. However, Defendant's promises are outright lies, designed to lull users into a false sense of security. Even after users elect to "Reject Advertising Cookies", Defendant surreptitiously enables several third parties – including Google LLC (DoubleClick and Google Analytics), Meta Platforms, Inc. (Facebook), Microsoft Corporation (Bing), Epsilon Data Management, LLC (Dotomi), Pinterest, Inc. (Pinterest), BlueConic, Inc., and others (the "Third

Parties") – to place and/or transmit cookies that track users' Websites browsing activities and eavesdrop on users' private communications on the Websites.

3. Contrary to their express rejection of cookies and tracking technologies on the Websites, Defendant nonetheless caused cookies, including the Third Parties' cookies, to be sent to Plaintiffs and other visitors' browsers, stored on their devices, and transmitted to the Third Parties along with user data. These third-party cookies permitted the Third Parties to track and collect data in real time regarding Websites visitors' behaviors and communications, including their browsing history, visit history, Website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

4. The Third Parties analyze and aggregate this user data across websites and time for their own purposes and financial gain, including, creating consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics; creating audience segments based on shared traits (such as Millennials, tech enthusiasts, etc.); and performing targeted advertising and marketing analytics. Further, the Third Parties share user data and/or user profiles to unknown parties to further their financial gain.

5. This type of tracking and data sharing is exactly what the Website visitors who clicked or selected the "Reject Advertising Cookies" button on the Websites' cookie consent banners sought to avoid. Defendant falsely told users of the Websites that it respected their privacy and that they could avoid tracking and data sharing when they browsed the Websites. Despite receiving notice of consumers' express declination of consent, Defendant defied it and violated state statutes, tort duties, and also breached its contractual duties and the implied covenant of good faith and fair dealing with Plaintiffs and those similarly situated users of the Websites.

THE PARTIES

6. Plaintiff Marco Walsh is, and was at all relevant times, an individual and resident of Scotts Valley, California. Plaintiff intends to remain in California and makes his permanent home there.

7. Plaintiff Howard Yosha is, and was at all relevant times, an individual and resident of Laguna Hills, California. Plaintiff intends to remain in California and makes his permanent home there.

8. Plaintiff Erica Maldonado is, and was at all relevant times, an individual and resident of Vista, California. Plaintiff intends to remain in California and makes his permanent home there.

9. Defendant Dollar Trees Stores, Inc. is a Virginia corporation with its headquarters and principal place of business in Chesapeake, Virginia.

JURISDICTION AND VENUE

10. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332(d)(2). The aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs; and Plaintiffs and Defendant are citizens of different states.

11. The injuries, damages and/or harm upon which this action is based, occurred or arose out of activities engaged in by Defendant within, affecting, and emanating from, the State of California. Defendant regularly conducts and/or solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products and services provided to persons in the State of California. Defendant has engaged, and continues to engage, in substantial and continuous business practices in the State of California.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in the state of California, including within this District.

13. Plaintiffs accordingly allege that jurisdiction and venue are proper in this Court.

SUBSTANTIVE ALLEGATIONS

A. Defendant Programmed the Websites to Include Third-Party Resources that Utilize Cookie Trackers.

14. Every website, including the Websites, is hosted by a server that sends and receives communications in the form of HTTP requests, such as "GET" or "POST" requests, to and from Internet users' browsers. For example, when a user clicks on a hyperlink on the Websites, the user's browser sends a "GET" request to the Website's server. The GET request tells the Website's server what information is being requested (e.g., the URL of the webpage being requested) and instructs the Website's server to send the information back to the user (e.g., the content of the webpage being requested). When the Website server receives an HTTP request, it processes that request and sends back an HTTP response. The HTTP request includes the client's IP address so that the Website server to knows where to send the HTTP response.

15. An IP address (Internet Protocol address) is a unique numerical label assigned to each device connected to a network that uses the Internet Protocol for communication, typically expressed as four sets of numbers separated by periods (e.g., 192.168.123.132 for IPv4 addresses). IP addresses can identify the network a device is on and the specific device within that network. Public IP addresses used for internet-facing devices reveal geographical locations, such as country, city, or region, through IP geolocation databases.

16. Defendant voluntarily integrated "third-party resources" from the Third Parties into its Websites' programming. "Third-party resources" refer to tools, content or services provided by third-parties, such as analytics tools, advertising networks, or payment processors, that a website developer utilizes by embedding scripts, styles, media, or application programming interface (API) into the Websites' code. Defendant's use of the third-party resources on the Websites is done so pursuant to agreements between Defendant and those Third Parties.

17. The Websites cause users' devices to store and/or transmit both first-party and third-party tracking cookies. Cookies are small text files sent by a website server to a user's web browser and stored locally on the user's device. As described below, cookies generally contain

a unique identifier which enables the website to recognize and differentiate individual users. Cookie files are sent back to the website server along with HTTP requests, enabling the website to identify the device making the requests, and to record a session showing how the user interacts with the website.

18. First-party cookies are those that are placed on the user's device directly by the web server with which the user is knowingly communicating (in this case, the Websites' server(s)). First-party cookies are used to track users when they repeatedly visit the same website.

19. A third-party cookie is set by a third-party domain/webserver (e.g., www.google.com; td.doubleclick.net; bing.com; pinterest.com, etc.). When the user's browser loads a webpage (such as a webpage of the Websites) containing embedded third-party resources, the third-parties' programming scripts typically issue HTTP commands to determine whether the third-party cookies are already stored on the user's device and to cause the user's browser to store those cookies on the device if they do not yet exist. Third-party cookies include an identifier that allows the third-party to recognize and differentiate individual users across websites (including the Websites) and across multiple browsing sessions.

20. As described further below, the third-party cookies stored on and/or loaded from users' devices when they interact with the Websites are transmitted to those third parties, enabling them to surreptitiously track in real time and collect Website users' personal information, such as their browsing activities and private communications with Defendant, including the following:

- **Browsing History**: Information about the webpages a Website user visits, including the URLs, titles, and keywords associated with the webpages viewed, time spent on each page, and navigation patterns;
- **Visit History**: Information about the frequency and total number of visits to the Website;
- **Website Interactions:** Data on which links, buttons, or ads on the Website that a user clicks;

- **User Input Data**: The information the user entered into the Website's form fields, including search queries, the user's name, age, gender, email address, location, and/or payment information;
- **Demographic Information**: Inferences about age, gender, and location based on browsing habits and interactions with Website content;
- **Interests and Preferences**: Insights into user interests based on the types of Website content viewed, products searched for, or topics engaged with;
- **Shopping Behavior**: Information about the Website products viewed or added to shopping carts;
- **Device Information**: Details about the Website user's device, such as the type of device (mobile, tablet, desktop), operating system, and browser type;
- **Referring URL**: Information about the Website that referred the user to the Website;
- **Session Information**: Details about the user's current Website browsing session, including the exact date and time of the user's session, the session duration and actions taken on the Website during that session;
- **User Identifiers**: A unique ID that is used to recognize and track a specific Website user across different websites over time; and/or
- **Geolocation Data**: General location information based on the Website user's IP address or GPS data, if accessible.

(Collectively, the browsing activities and private communications listed in the bullet points above shall be referred to herein as "Private Communications").

21. Third-party cookies can be used for a variety of purposes, including (i) analytics (e.g., tracking and analyzing visitor behavior, user engagement, and effectiveness of marketing campaigns); (ii) personalization (e.g., remembering a user's browsing history and purchase preferences to enable product recommendations); (iii) advertising/targeting (e.g., delivering targeted advertisements based on the user's consumer profile (i.e., an aggregated profile of the

user's behavior, preferences, and demographics); and (iv) social media integration (e.g., enabling sharing of users' activities with social media platforms). Ultimately, third-party cookies are utilized to boost Websites performance and revenue through the collection, utilization, and dissemination of user data.

22. Defendant specializes in retail, primarily offering affordable household goods, seasonal items, and general consumer merchandise through its brands Dollar Tree and Family Dollar. Defendant also owns and operates the Websites, which allows visitors to receive information about its products, locate retail stores, and purchase products. As they interact with the Websites (e.g., by entering data into forms, clicking on links, and making selections), Website users communicate Private Communications to Defendant, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

23. Defendant chose to install or integrate the Websites with resources from the Third Parties that, among other things, use cookies. Thus, when consumers visit the Websites, both first-party cookies and third-party cookies are placed on their devices and/or transmitted. This is caused by software code that Defendant incorporates into the Websites, or that Defendant causes to be loaded. Because Defendant controls the software code of the Websites, it has complete control over whether first-party and third-party cookies are placed on its users' devices and/or transmitted to third parties.

24. Defendant explained the third-party cookies it used on the Websites as follows in the Dollar Tree Website "Manage Cookies" link in the cookie consent banner:

> Site Cookie Preferences
>
> When you visit our website, we store cookies on your browser to collect information. The information collected might relate to you, your preferences, or your device, and is mostly used to make the site work as you expect it to and to provide a more personalized web experience. However, you can choose to block certain types of cookies, which may impact your experience of the site and the services we are able to offer. For more information about our privacy practices, please see our Privacy Policy.

> Advertising Cookies
>
> These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant information on other sites. They are based on uniquely identifying your browser and internet device. You can place the toggle above to the right to opt in to these activities on this digital property consistent with applicable law. Please note that, because these activities are based on online cookies, your choice is specific to this property.

25. Defendant further explained the third-party cookies it used on the Dollar Tree Website as follows in the Dollar Tree Privacy Policy[1]:

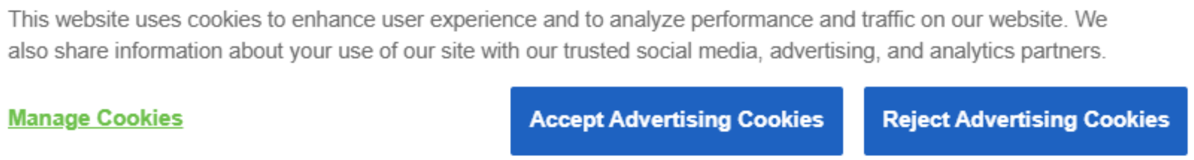
> We participate in behavior-based advertising, which means that a third-party uses technology (e.g., a cookie) to collect information about your use of our Site so that they can provide advertising about products and Services tailored to your interests on our Site, or on other websites. For more information relating to the use of such tools, review the section entitled Cookies and Online Interactions.
>
> …
>
> COOKIES AND ONLINE INTERACTIONS
>
> We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs (collectively, "Cookies"). Cookies are small bits of data cached or stored on your computer or mobile device based on your Internet activity…
>
> **Essential Cookies**
>
> These are cookies that the Services need in order to function, and that enable you to move around and use the Services and features. Without these essential cookies, the Services will not perform as smoothly for you as we would like it to and we may not be able to provide the Services or certain Services or features you request. Examples of where these cookies are used include: to determine when you are signed in; to determine when your account has been inactive; and for other troubleshooting and security purposes.
>
> **Analytics Cookies**
>
> Analytics cookies allow us to understand more about how many visitors we have to our Services, how many times they visit us and how many times a user viewed specific pages within our Services. Although analytics cookies allow us to gather specific information about the pages that you visit and whether you have visited

[1] Dollar Tree Privacy Policy (Last Updated Date: October 16, 2023) (current version available at https://www.dollartree.com/privacy-policy) (the "Privacy Policy"). Defendant has subsequently updated its Privacy Policy, but based on information and belief, this is the version that was in effect when Plaintiffs initially rejected advertising cookies on the Website.

> our Services multiple times, we cannot use them to find out details such as your name or address. We use Google Analytics…
>
> Advertising Cookies
>
> Depending on your location and in certain circumstances, Dollar Tree may work with third- party online or mobile network advertisers that use cookies to help us manage advertising. These cookies may enable third-party ad networks to recognize a unique cookie on your computer or mobile device and may be placed by us or our network advertising firm that works with our third-party network advertiser. The information that is collected and shared by cookies may be linked to the device identifier of the device you are using to allow us to keep track of all the sites and mobile applications you have visited that are associated with the ad network. This information may be used for the purpose of targeting advertisements on the Dollar Tree Services and third-party sites or mobile applications based on those interests. The information collected by these cookies may also be used to allow us to analyze the effectiveness of our advertisements.

B. <u>Defendant Falsely Informed Users That They Could Reject the Websites' Use of Advertising Cookies.</u>

26. When consumers in California visited the Websites, the Websites immediately displayed to them a popup cookie consent banner. As shown in the screenshot below, the cookie consent banner stated, “This website uses cookies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our trusted social media, advertising, and analytics partners.” The banner then purported to provide users the opportunity to “Reject Advertising Cookies” as shown, in the following screenshot from the Dollar Tree Website. An identical cookie consent banner is displayed on the Family Dollar Website.



This website uses cookies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our trusted social media, advertising, and analytics partners.

27. Website users who clicked or selected the “Reject Advertising Cookies” button, indicating their choice and/or agreement to decline or reject advertising cookies and tracking technologies in use on the Websites, could then continue to browse the Websites, and the popup cookie consent banner disappeared.

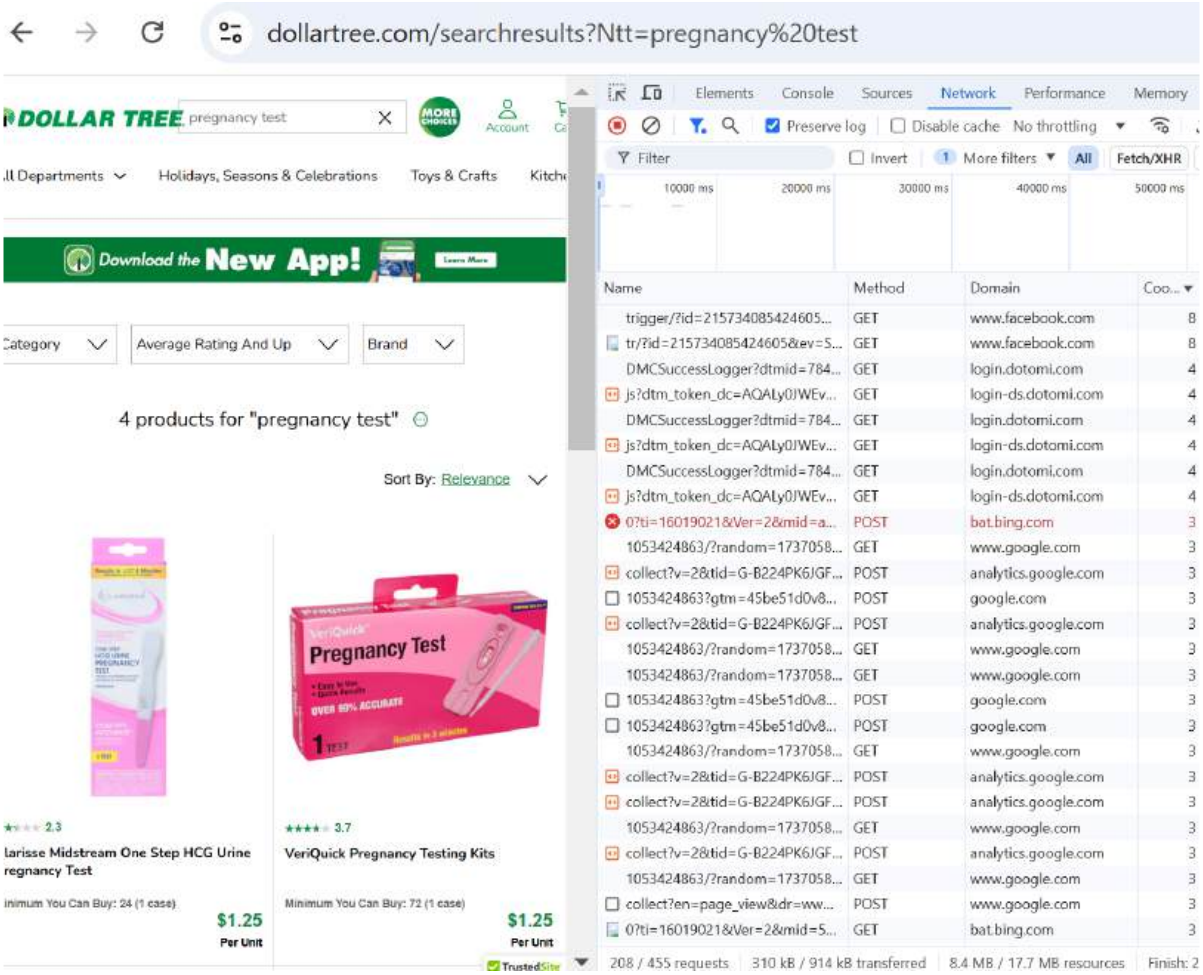
28. Defendant's popup cookie consent banner led Plaintiffs, and all those users of the Websites similarly situated, to believe that they declined or rejected advertising cookies and tracking technologies. The banner further reasonably led Plaintiffs and users of the Websites similarly situated to believe that Defendant would not allow third parties, through cookies, to access their Private Communications with the Websites, including their browsing history, visit history, Website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, upon clicking or selecting the "Reject Advertising Cookies" button.

29. Defendant's representations, however, were false. In truth, Defendant did not abide by its users' wishes. When users clicked the "Reject Advertising Cookies" button, they provided notice to Defendant that they did not consent to the placement or transmission of third-party advertising cookies that would allow those parties to obtain their Private Communications with the Websites. Nevertheless, Defendant caused the Third-Party advertising and/or tracking cookies to be placed on Website users' browsers and devices and/or transmitted to the Third Parties along with user data.

30. In particular, when users clicked or selected the "Reject Advertising Cookies" button, Defendant nonetheless continued to cause the Third Parties' cookies to be placed on users' devices and/or transmitted to the Third Parties along with user data, enabling them to collect user data in real time that discloses Website users' Private Communications, including browsing history, visit history, Website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data. In other words, even when consumers like Plaintiffs tried to protect their privacy by rejecting cookies, Defendant failed to prevent cookies from being transmitted to Third Parties, enabling them to track user behavior and communications.

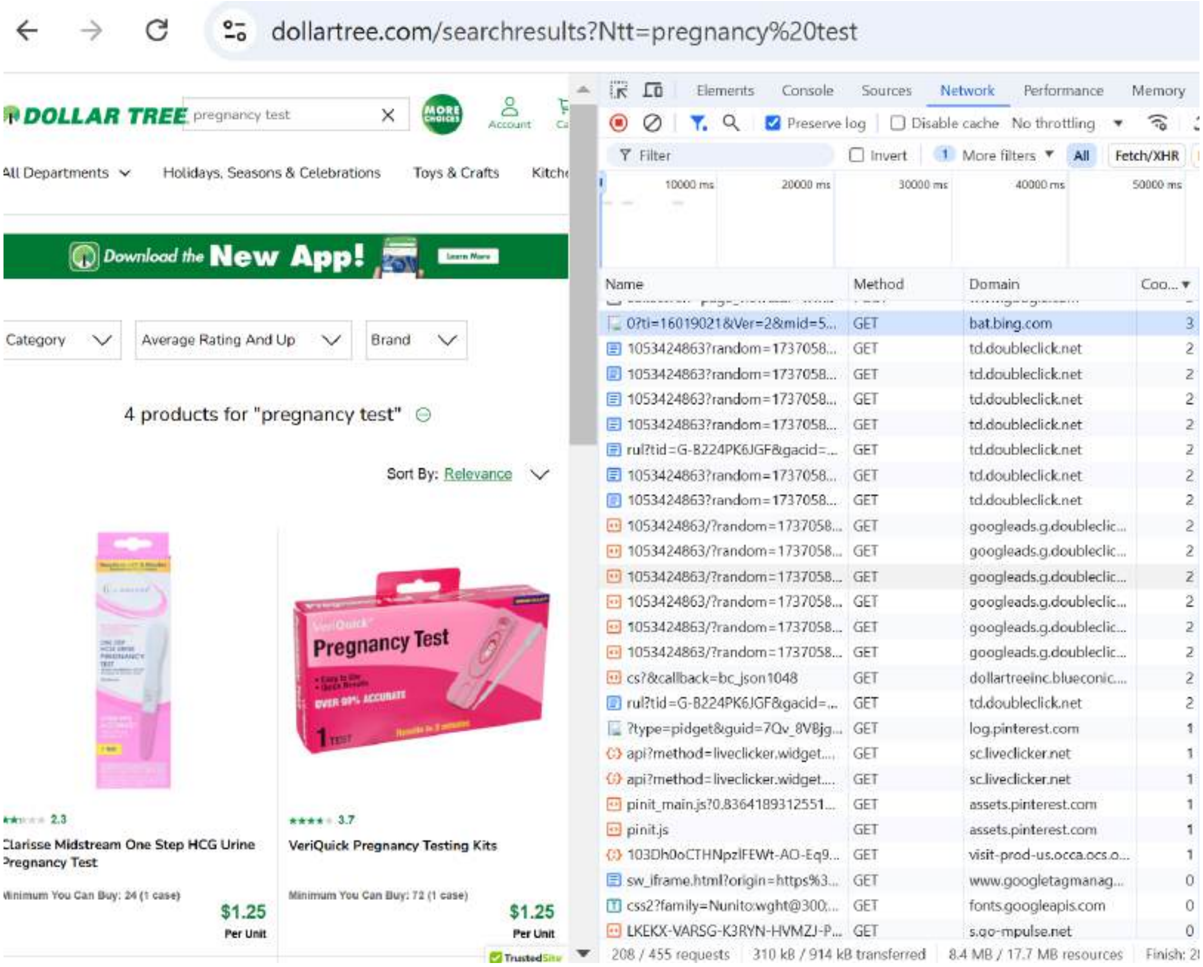
31. Some aspects of the operations of the Third-Party cookies on the Websites can be observed using specialized tools that log incoming and outgoing website network transmissions. The following screenshots, obtained using one such tool, show examples of Third-Party cookies being transmitted from a Dollar Tree Website user's device and browser to Third Parties even after the user clicked the "Reject Advertising Cookies" button in the popup cookie consent banner.

[REMAINDER OF PAGE INTENTIONALLY BLANK]



Name	Method	Domain	Coo... ▾
trigger/?id=215734085424605...	GET	www.facebook.com	8
tr/?id=215734085424605&ev=S...	GET	www.facebook.com	8
DMCSuccessLogger?dtmid=784...	GET	login.dotomi.com	4
js?dtm_token_dc=AQALy0JWEv...	GET	login-ds.dotomi.com	4
DMCSuccessLogger?dtmid=784...	GET	login.dotomi.com	4
js?dtm_token_dc=AQALy0JWEv...	GET	login-ds.dotomi.com	4
DMCSuccessLogger?dtmid=784...	GET	login.dotomi.com	4
js?dtm_token_dc=AQALy0JWEv...	GET	login-ds.dotomi.com	4
0?ti=16019021&Ver=2&mid=a...	POST	bat.bing.com	3
1053424863/?random=1737058...	GET	www.google.com	3
collect?v=2&tid=G-B224PK6JGF...	POST	analytics.google.com	3
1053424863?gtm=45be51d0v8...	POST	google.com	3
collect?v=2&tid=G-B224PK6JGF...	POST	analytics.google.com	3
1053424863/?random=1737058...	GET	www.google.com	3
1053424863/?random=1737058...	GET	www.google.com	3
1053424863?gtm=45be51d0v8...	POST	google.com	3
1053424863?gtm=45be51d0v8...	POST	google.com	3
1053424863/?random=1737058...	GET	www.google.com	3
collect?v=2&tid=G-B224PK6JGF...	POST	analytics.google.com	3
collect?v=2&tid=G-B224PK6JGF...	POST	analytics.google.com	3
1053424863/?random=1737058...	GET	www.google.com	3
collect?v=2&tid=G-B224PK6JGF...	POST	analytics.google.com	3
1053424863/?random=1737058...	GET	www.google.com	3
collect?en=page_view&dr=ww...	POST	www.google.com	3
0?ti=16019021&Ver=2&mid=5...	GET	bat.bing.com	3

208 / 455 requests | 310 kB / 914 kB transferred | 8.4 MB / 17.7 MB resources | Finish: 2



Name	Method	Domain	Coo...
0?ti=16019021&Ver=2&mid=5...	GET	bat.bing.com	3
1053424863?random=1737058...	GET	td.doubleclick.net	2
1053424863?random=1737058...	GET	td.doubleclick.net	2
1053424863?random=1737058...	GET	td.doubleclick.net	2
1053424863?random=1737058...	GET	td.doubleclick.net	2
rul?tid=G-B224PK6JGF&gacid=...	GET	td.doubleclick.net	2
1053424863?random=1737058...	GET	td.doubleclick.net	2
1053424863?random=1737058...	GET	td.doubleclick.net	2
1053424863/?random=1737058...	GET	googleads.g.doubleclic...	2
1053424863/?random=1737058...	GET	googleads.g.doubleclic...	2
1053424863/?random=1737058...	GET	googleads.g.doubleclic...	2
1053424863/?random=1737058...	GET	googleads.g.doubleclic...	2
1053424863/?random=1737058...	GET	googleads.g.doubleclic...	2
1053424863/?random=1737058...	GET	googleads.g.doubleclic...	2
cs?&callback=bc_json1048	GET	dollartreeinc.blueconic....	2
rul?tid=G-B224PK6JGF&gacid=...	GET	td.doubleclick.net	2
?type=pidget&guid=7Qv_8VBjg...	GET	log.pinterest.com	1
api?method=liveclicker.widget....	GET	sc.liveclicker.net	1
api?method=liveclicker.widget....	GET	sc.liveclicker.net	1
pinit_main.js?0.8364189312551...	GET	assets.pinterest.com	1
pinit.js	GET	assets.pinterest.com	1
103Dh0oCTHNpzlFEWt-AO-Eq9...	GET	visit-prod-us.occa.ocs.o...	1
sw_iframe.html?origin=https%3...	GET	www.googletagmanag...	0
css2?family=Nunito:wght@300;...	GET	fonts.googleapis.com	0
LKEKX-VARSG-K3RYN-HVMZJ-P...	GET	s.go-mpulse.net	0

208 / 455 requests | 310 kB / 914 kB transferred | 8.4 MB / 17.7 MB resources | Finish: 2

32. The screenshots above show the "Network" tab of Chrome Developer Tools, which contains a list of HTTP network traffic transmissions between the user's browser and various third-party websites while the user visited and interacted with Defendant's Website at https://www.dollartree.com. The screenshots depict only network traffic occurring ***after*** the user rejected advertising cookies using the cookie banner. As shown above, despite the user's rejection of advertising cookies, the user's interactions with the Websites resulted in the user's browser making a large number of GET and POST HTTP requests to third party web domains like analytics.google.com, www.google.com, td.doubleclick.net, www.facebook.com, and others. As further shown in the right-hand column of the screenshots, the user's browser sent cookies along with those HTTP requests to the third parties. These screenshots demonstrate that the Websites caused third-party cookie data and users' Private Communications to be

transmitted to Third Parties, even after consumers declined or rejected advertising cookies and tracking technologies by clicking or selecting the "Reject Advertising Cookies" button. All of these network calls are made to the Third Parties without the user's knowledge, and despite the user's rejection of advertising cookies.

33. The Family Dollar Website similarly cause consumers' devices to transmit user data to third parties—even after consumers reject cookies by clicking the "Reject Advertising Cookies" button—on the Website's cookie consent banner.

34. Website users' Private Communications, including their browsing history, visit history, Website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, are surreptitiously obtained by the Third Parties via these cookies.

35. As users interact with the Websites, even after clicking or selecting the "Reject Advertising Cookies" button, thereby declining or rejecting the use of advertising cookies and similar technologies for personalized content and advertising, and as well as the sale or sharing of the user's personal information with third parties for such functions, more data regarding users' behavior and communications are sent to third parties, alongside the cookie data. The third-party cookies that Defendant wrongfully allows to be stored on users' devices and browsers, and to be transmitted to the Third Parties, enable the Third Parties to track and collect data on users' behaviors and communications, including Private Communications, on the Websites. Because third-party cookies enable Third Parties to track users' behavior across the Internet and across time, user data can be correlated and combined with other data sets to compile comprehensive user profiles that reflect consumers' behavior, preferences, and demographics (including psychological trends, predispositions, attitudes, intelligence, abilities, and aptitudes). These Third-Parties monetize user profiles for advertising, sales, and marketing purposes to generate revenue and target advertising to Internet users. Advertisers can gain deep

understanding of users' behavioral traits and characteristics and target those users with advertisements tailored to their consumer profiles and audience segments.

36. The Third-Party code that the Websites cause to be loaded and executed by the user's browser becomes a wiretap when it is executed because it enables the Third Parties—separate and distinct entities from the parties to the conversations—to use cookies to eavesdrop upon, record, extract data from, and analyze conversations to which they are not parties. When the Third Parties use their respective wiretaps on Website users' Private Communications, the wiretaps are not like tape recorders or "tools" used by one party to record the other. The Third Parties each have the capability to use the contents of conversations they collect through their respective wiretaps for their own purposes as described in more detail below.

C. <u>Defendant's Conduct Violated Its Own Privacy Policy.</u>

37. Defendant's aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties to track users' Private Communications on the Websites using third-party cookies—even after those users click or select the "Reject Advertising Cookies" button—is particularly egregious given Defendant's additional written assurances in its Privacy Policy that users can, in fact, opt out of cookies and tracking technologies used on the Website. Specifically, Defendant represented to Plaintiff and its users the following in the Privacy Policy:

> In addition, depending on your location and applicable laws, we may give you the option of adjusting your preferences regarding the categories of Cookies we use. When this option is available, you can configure your personal settings on our 'Manage Cookies' or via other options that may be available on the relevant Service.

D. <u>The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting Defendant's Websites.</u>

1. Google Cookies

38. Defendant causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users reject advertising cookies to and from the **<u>www.google.com, analytics.google.com, and doubleclick.net</u>** domains. Each of these domains

is associated with Google LLC's digital advertising and analytics platform that collects user information via cookies to assist Google in performing data collection, behavioral analysis, user retargeting, and analytics.[2] Google serves targeted ads to web users across Google's ad network, which spans millions of websites and apps. Nearly 20% of web traffic is tracked by Google's DoubleClick cookies.[3] Google's cookies help it track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. Further, by identifying users who have shown interest in certain products or content, Google's cookies enable its advertising platform to enable advertisers to show relevant ads to those users when they visit other websites within Google's ad network.[4]

39. Specifically, Google sends cookies when a web user visits a webpage that shows Google Marketing Platform advertising products and/or Google Ad Manager ads.[5] "Pages with Google Marketing Platform advertising products or Google Ad Manager ads include ad tags that instruct browsers to request ad content from [Google's] servers. When the server delivers the ad content, it also sends a cookie. But a page doesn't have to show Google Marketing Platform advertising products or Google Ad Manager ads for this to happen; it just needs to include Google Marketing Platform advertising products or Google Ad Manager ad tags, which might load a click tracker or impression pixel instead." *Id.* As Google explains, "Google Marketing

[2] *See* Our advertising and measurement cookies (available at https://business.safety.google/adscookies/).

[3] *See, e.g.* https://www.ghostery.com/whotracksme/trackers/doubleclick.

[4] *See, e.g.* About cross-channel remarketing in Search Ads 360 (available at https://support.google.com/searchads/answer/7189623?hl=en); About dynamic remarketing for retail (available at https://support.google.com/google-ads/answer/6099158?hl=en&sjid=1196213575075458908-NC).

[5] *See* How Google Marketing Platform advertising products and Google Ad Manager use cookies (available at https://support.google.com/searchads/answer/2839090?hl=en&sjid=1196213575075458908-NC); *see also* Cookies and user identification (available at https://developers.google.com/tag-platform/security/concepts/cookies).

Platform advertising products and Google Ad Manager send a cookie to the browser after any impression, click, or other activity that results in a call to our servers." *Id.*

40. Google also uses cookies in performing analytical functions. As Google explains, "Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights into [] business[es]."[6] "To measure a website … [one] add[s] a small piece of JavaScript measurement code to each page on [a] site." *Id.* Then, "[e]very time a user visits a webpage, the tracking code will collect … information about how that user interacted with the page." *Id.* Google Analytics enables website owners to "measure when someone loads a page, clicks a link, [ ] makes a purchase;" "completes a purchase"; "searches [] website or app"; "select content on [] website or app"; "views an item"; and "views their shopping cart."[7]

41. Google's cookies allow it to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data.[8]

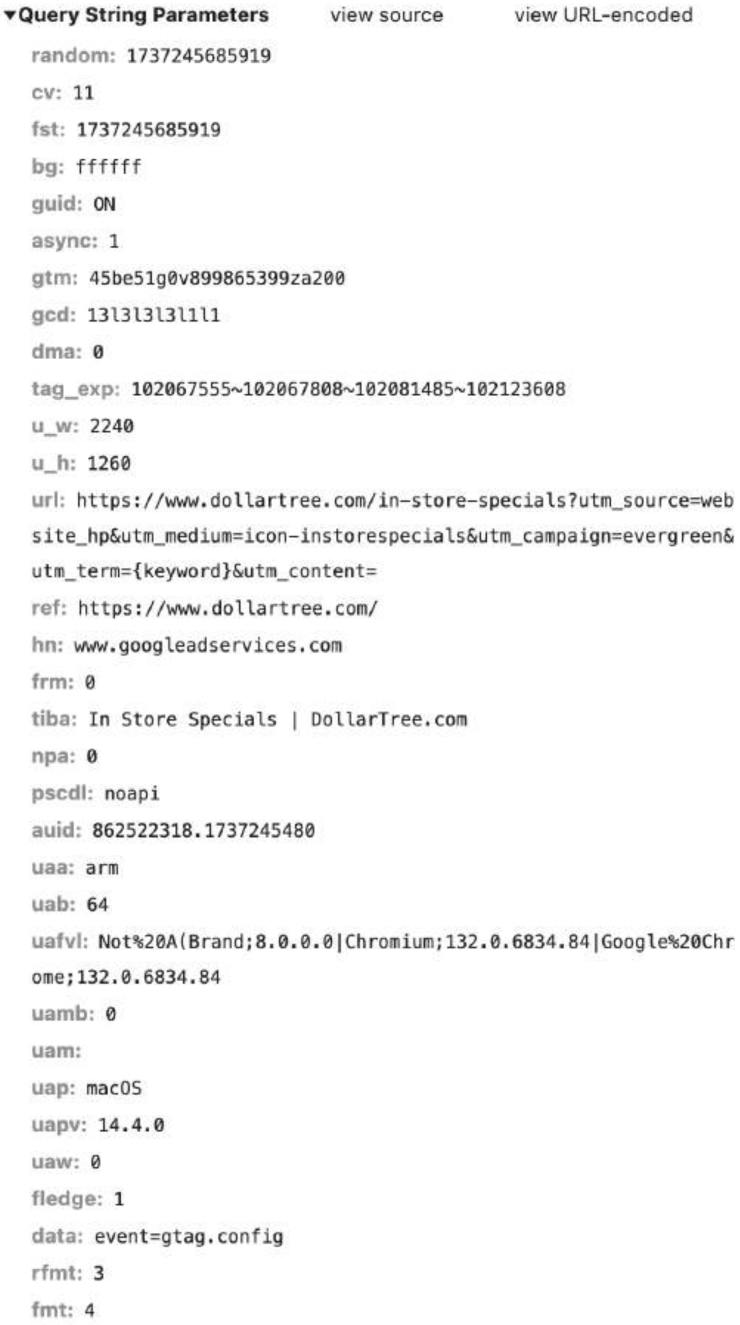
[6] How Google Analytics Works (available at https://support.google.com/analytics/answer/12159447?hl=en).

[7] _Set up events (available at https://developers.google.com/analytics/devguides/collection/ga4/events); and Recommended events (available at https://developers.google.com/analytics/devguides/collection/ga4/events).

[8] *See* About the Google Tag (available at https://support.google.com/searchads/answer/7550511?hl=en); How Floodlight Recognizes Users (available at https://support.google.com/searchads/answer/2903014?hl=en); How Google Ads tracks website conversions (available at https://support.google.com/google-ads/answer/7521212); Google Ads Help, Cookie: Definition (available at https://support.google.com/google-ads/answer/2407785?hl=en); About demographic targeting in Google Ads (available at https://support.google.com/searchads/answer/7298581?hl=en&sjid=11962135750754589O8-NC&visit_id=638670675669576522-2267083756&ref_topic=7302618&rd=1); How Google Analytics Works (https://support.google.com/analytics/answer/12159447); Set up events (available at https://developers.google.com/analytics/devguides/collection/ga4/events); and Recommended events (available at https://support.google.com/analytics/answer/9267735).

42. For example, the Google software code that Defendant causes to be stored on and executed by the Website user's device causes the following data to be sent to Google's domain, at https://googleads.g.doubleclick.net:

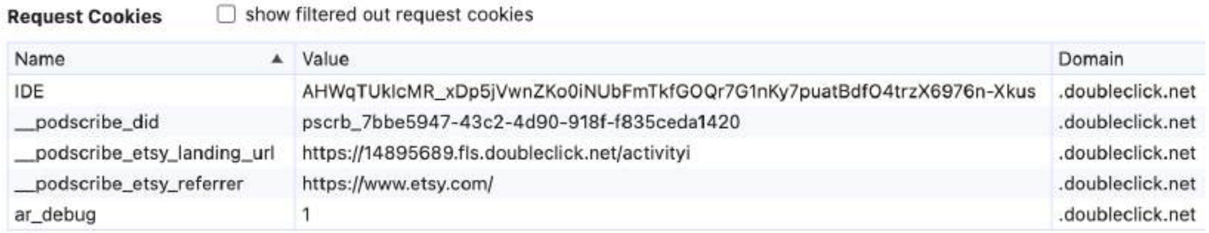
[REMAINDER OF PAGE INTENTIONALLY BLANK]



```
▾Query String Parameters      view source      view URL-encoded
  random: 1737245685919
  cv: 11
  fst: 1737245685919
  bg: ffffff
  guid: ON
  async: 1
  gtm: 45be51g0v899865399za200
  gcd: 13l3l3l3l1l1
  dma: 0
  tag_exp: 102067555~102067808~102081485~102123608
  u_w: 2240
  u_h: 1260
  url: https://www.dollartree.com/in-store-specials?utm_source=web
  site_hp&utm_medium=icon-instorespecials&utm_campaign=evergreen&
  utm_term={keyword}&utm_content=
  ref: https://www.dollartree.com/
  hn: www.googleadservices.com
  frm: 0
  tiba: In Store Specials | DollarTree.com
  npa: 0
  pscdl: noapi
  auid: 862522318.1737245480
  uaa: arm
  uab: 64
  uafvl: Not%20A(Brand;8.0.0.0|Chromium;132.0.6834.84|Google%20Chr
  ome;132.0.6834.84
  uamb: 0
  uam:
  uap: macOS
  uapv: 14.4.0
  uaw: 0
  fledge: 1
  data: event=gtag.config
  rfmt: 3
  fmt: 4
```

43. Among this data is the "url" parameter, which tells Google the exact page on the website that the user was visiting (in this case, the "in store specials" page).

44. Along with this data, the Google software code that Defendant causes to be stored on and executed by the user's device causes the following cookies to be sent to Google's domain:

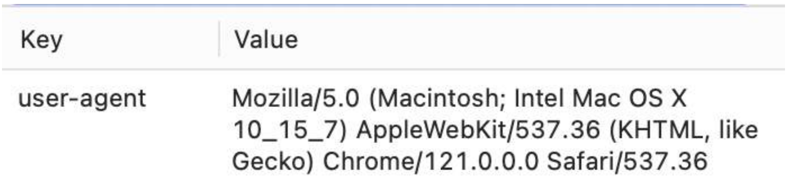


Request Cookies □ show filtered out request cookies

Name ▲	Value	Domain
IDE	AHWqTUkIcMR_xDp5jVwnZKo0iNUbFmTkfGOQr7G1nKy7puatBdfO4trzX6976n-Xkus	.doubleclick.net
__podscribe_did	pscrb_7bbe5947-43c2-4d90-918f-f835ceda1420	.doubleclick.net
__podscribe_etsy_landing_url	https://14895689.fls.doubleclick.net/activityi	.doubleclick.net
__podscribe_etsy_referrer	https://www.etsy.com/	.doubleclick.net
ar_debug	1	.doubleclick.net

45. As confirmed by Google's documentation, the IDE cookie is a tracking and identification cookie "used to show Google ads on non-Google sites" and "to personalize the ads [users] see."

46. Along with all of this data, the user's browser additionally sends the "user-agent" to Google:



Key	Value
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

47. The "user-agent" corresponds to the device and browser that the user has used to access the Dollar Tree Website. In this case, the user-agent value corresponds to Google's Chrome browser version 121, running on the Catalina version of macOS.[9]

48. Finally, the data sent to Google contains the user's IP address.

49. Because Google's cookies operate across multiple sites (i.e., cross-site tracking), the cookie enables Google to track users as they navigate from one site to another, and to comprehensively observe and evaluate user behavior online. Google's advertising platform aggregates user data to create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics and audience segments based on shared

[9] There are many tools on the web that are capable of parsing user-agent strings to determine what browser and operating system they pertain to. One such tool is located at https://explore.whatismybrowser.com/useragents/parse.

traits (such as females, Millennials, etc.), and to perform targeted advertising and marketing analytics.

50. Thus, the Google cookies used on the Websites enable Google to track users' interactions with advertisements to help advertisers understand how users engage with ads across different websites. Further, the user data collected through the cookie enables the delivery of personalized ads based on user interests and behaviors. For instance, if a user frequently visits travel-related websites, Google will show her more travel-related advertisements. Further, the collected data is used to generate reports for advertisers, helping them assess the performance of their ad campaigns and make data-driven decisions (such as renaming their products). Further, Google's advertising platform enables advertisers to retarget marketing, which Google explains allows advertisers to "show previous visitors ads based on products or services they viewed on your website. With messages tailored to your audience, dynamic remarketing helps you build leads and sales by bringing previous visitors back to your website to complete what they started."[10]

51. Further, in its "Shared Data Under Measurement Controller-Controller Data Protection Terms," Google states: "Google can access and analyze the Analytics data customers share with us to better understand online behavior and trends, and improve our products and services—for example, to improve Google search results, detect and remove invalid advertising traffic in Google Ads, and test algorithms and build models that power services like Google Analytics Intelligence that apply machine-learning to surface suggestions and insights for customers based on their analytics data and like Google Ads that applies broad models to improve ads personalization and relevance. These capabilities are critical to the value of the products we deliver to customers today."[11] Thus, Google can have the capability to use the data it collects for understanding online behavior and trends, machine learning, and improving its own products and services.

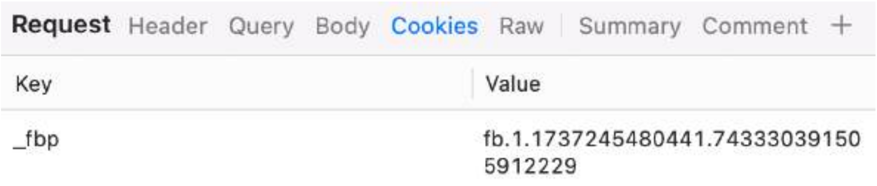
[10] Dynamic remarketing for web setup guide (available at https://support.google.com/google-ads/answer/6077124).

[11] Shared Data Under Measurement Controller-Controller Data Protection Terms (available at https://support.google.com/analytics/answer/9024351).

2. Facebook Cookies

52. Defendant also cause third party cookies to be transmitted to and from Website users' browsers and devices to and from the **<u>facebook.com</u>** domain, even after users elect to reject advertising cookies. This domain is associated with Meta's digital advertising and analytics platform that collects user information via cookies to assist Meta in performing data collection, behavioral analysis, user retargeting, and analytics.[12] Meta serves targeted ads to web users across Meta's ad network, which spans millions of websites and apps.

53. The facebook.com cookies help Meta track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. As the user browses and interacts with the Websites, the Facebook code installed by Defendant on the user's browser repeatedly causes the browser to transmit the "_fbp" cookie, such as the following:



Key	Value
_fbp	fb.1.1737245480441.74333039150 5912229

54. Facebook's documentation states that "the '_fbp' cookie identifies browsers for the purposes of providing advertising and site analytics services…."[13] In fact, the "_fbp" cookie enables Facebook to identify the specific user's unique ID, which is associated with their Facebook profile. This ID enables Facebook to track user interactions on its platform and across sites that use Facebook plugins, such as adding items to a cart, clicking "Like" buttons, or engaging with comment sections. When combined with other data sent to the Facebook domain, this cookie allows Meta to track users' browsing activities. Facebook uses this data for various purposes, such as personalizing content, enhancing ad targeting accuracy, and refining its user experience.

[12] https://www.facebook.com/privacy/policies/cookies/.

[13] https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3

55. In particular, by identifying users who have shown interest in certain products or content, the facebook.com cookies enable Meta's advertising platform to enable advertisers to show relevant ads to those users when they visit other websites within Meta's ad network.[14] These cookies allow Meta to collect data on how users interact with websites, regardless of whether they have a Facebook account or are logged in.[15]

56. Further, along with all of this data, the Facebook software code that Defendant cause to be stored on and executed by the user's device causes the user's "user-agent" information to be sent to Meta.

57. The facebook.com cookies allow Meta to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data (including IP addresses).[16]

58. Meta utilizes the data collected through the facebook.com cookies for its own purposes, including by using the data to tailor content and target advertisements to users. This includes practices such as (i) **Ad Targeting and Retargeting**, in which Meta uses the facebook.com cookie to track users' online behavior across different sites, building a profile based on their browsing habits, purchases, and interactions. This profile enables Facebook to deliver highly targeted ads within the Facebook ecosystem and on other sites that are part of Facebook's Audience Network; (ii) **Conversion Tracking**, in which Meta uses the facebook.com cookie to enable business partners to track specific actions users take after viewing or clicking on a Facebook ad, such as making a purchase or signing up for a newsletter; (iii) **Audience Insights and Analytics**, in which Meta uses the facebook.com cookie to provide data to businesses on user demographics, interests, and behaviors across their sites and apps; and (iv) **Cross-Device and Cross-Platform Tracking**, in which Meta uses the facebook.com cookie

[14] *Id.*; https://allaboutcookies.org/what-data-does-facebook-collect

[15] https://allaboutcookies.org/what-data-does-facebook-collect.

[16] *Id.*

to support tracking users across devices and platforms, so that ads are targeted consistently regardless of the device a user is on. This ensures that advertisers can follow users across devices.

3. Microsoft Bing Cookies

59. Defendant also causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users elect to reject advertising cookies, to and from the **bat.bing.com** domain. "The webpage bat.bing.com is a host for Bing Ads Conversion tracking code. This webpage is owned by Microsoft[.]"[17] The domain is associated with Bing, Microsoft's search engine, as well as Microsoft's digital advertising and analytics platforms. When a webpage loads a bat.bing.com cookie, it "tells Microsoft Advertising about the user visits to [the] webpage."[18] Microsoft uses bat.bing.com cookies to "record[] what customers do on [a] website and send[] that information to Microsoft Advertising." [19] Microsoft then serves targeted ads to web users across its extensive ad networks, which utilizes its "rich" supply of gathered data to "reach more than a billion people[.]"[20]

60. Bat.bing.com cookies collect consumers' (i) search history and browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information (including zip code[21]; gender[22]; age[23] (including identifying whether that person is a minor or not)); (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data (including IP addresses). Bat.bing.com updates this information each time a user clicks on a

[17] https://answers.microsoft.com/en-us/msadvs/forum/all/does-batbing-track-your-browser-searches-and-sites/0a402f00-60c2-4d54-bd7d-81b67ccc7f13.

[18]https://help.ads.microsoft.com/apex/index/3/en/56959#:~:text=The%20most%20important%20request%20is,making%20when%20your%20webpage%20loads.

[19] https://help.ads.microsoft.com/#apex/ads/en/56960/1.

[20] https://answers.microsoft.com/en-us/msadvs/forum/all/opt-out-of-audience-ads/753bc0fc-c04f-4e20-a94a-abaa950ccf31#:~:text=When%20you%20come%20to%20Microsoft,and%20rich%20first%2Dparty%20data.

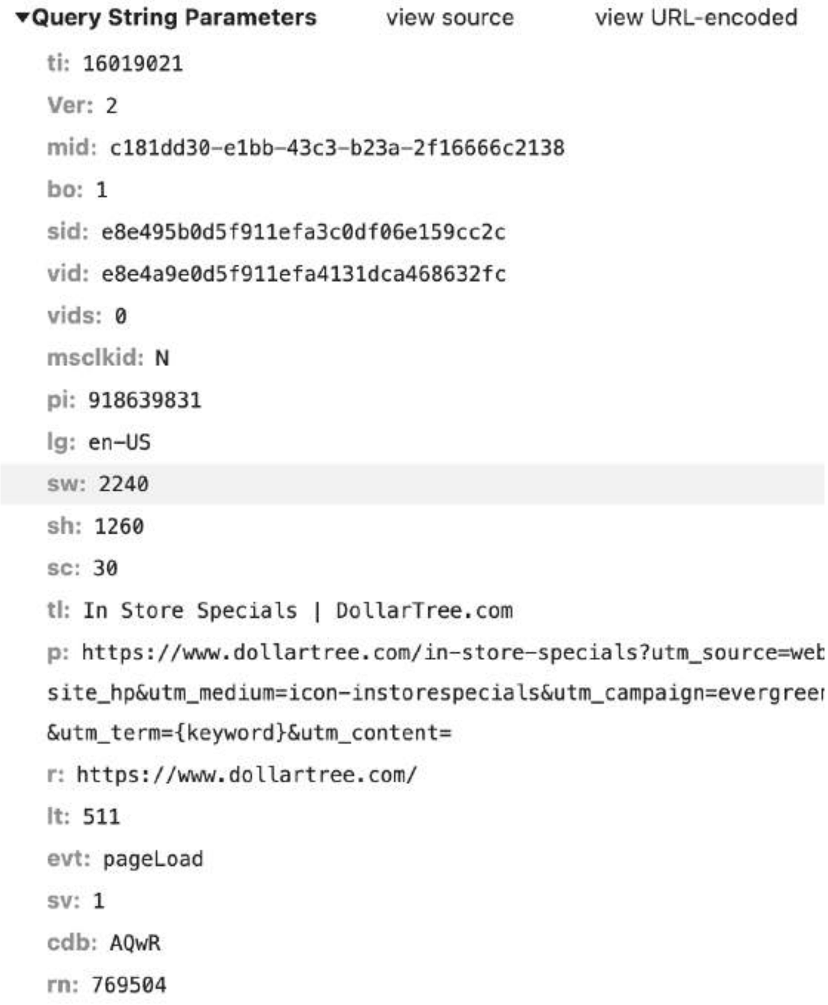
[21] https://help.ads.microsoft.com/#apex/ads/en/60212/0.

[22] *Id.*

[23] *Id.*

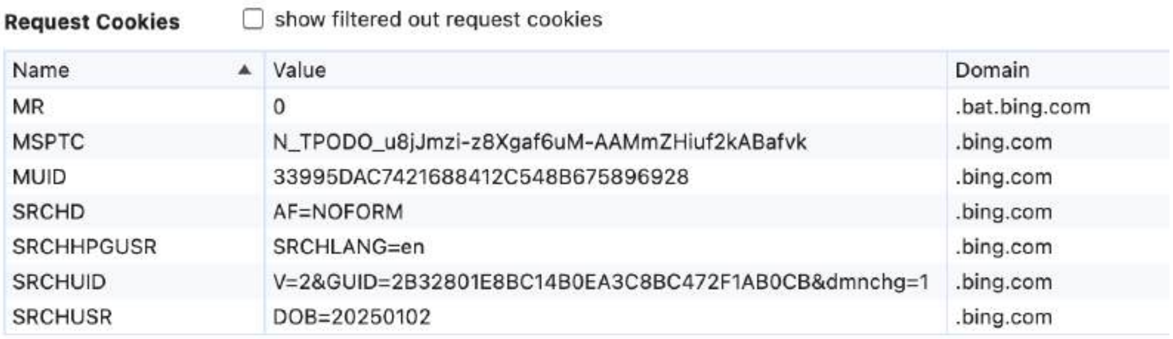
website hosting a third-party bat.bing.com cookie. Bat.bing.com keeps this user data for six months.

61. For example, even after rejecting cookies, when a user searches the Website for the phrase "pregnancy test," that search phrase is sent to Microsoft Bing, along with various other user data:



```
▾Query String Parameters      view source      view URL-encoded
  ti: 16019021
  Ver: 2
  mid: c181dd30-e1bb-43c3-b23a-2f16666c2138
  bo: 1
  sid: e8e495b0d5f911efa3c0df06e159cc2c
  vid: e8e4a9e0d5f911efa4131dca468632fc
  vids: 0
  msclkid: N
  pi: 918639831
  lg: en-US
  sw: 2240
  sh: 1260
  sc: 30
  tl: In Store Specials | DollarTree.com
  p: https://www.dollartree.com/in-store-specials?utm_source=web
  site_hp&utm_medium=icon-instorespecials&utm_campaign=evergreen
  &utm_term={keyword}&utm_content=
  r: https://www.dollartree.com/
  lt: 511
  evt: pageLoad
  sv: 1
  cdb: AQwR
  rn: 769504
```

62. Along with this data, cookies are sent to Microsoft Bing, such as the following:



Request Cookies □ show filtered out request cookies

Name ▲	Value	Domain
MR	0	.bat.bing.com
MSPTC	N_TPODO_u8jJmzi-z8Xgaf6uM-AAMmZHiuf2kABafvk	.bing.com
MUID	33995DAC7421688412C548B675896928	.bing.com
SRCHD	AF=NOFORM	.bing.com
SRCHHPGUSR	SRCHLANG=en	.bing.com
SRCHUID	V=2&GUID=2B32801E8BC14B0EA3C8BC472F1AB0CB&dmnchg=1	.bing.com
SRCHUSR	DOB=20250102	.bing.com

63. The MUID cookie value is a marketing cookie, used by Microsoft as a unique ID to enable tracking the user's device across the large number of Microsoft-affiliated websites on the internet.

64. Bat.bing.com cookies help Microsoft track users' interactions with ads (e.g., clicking a link or making a purchase) and provide valuable metrics that advertisers use to measure ad campaign performance. Further, bat.bing.com cookies allow Microsoft to obtain and store at user data to "help [website owners] focus a campaign or ad group on potential audiences who meet [website owners'] specific criteria, so [website owners] can increase the chance that [consumers] see [website owners'] ads."[24] Further, bat.bing.com offers [website owners] valuable "conversion tracking," which is a "measure [of] the ROI (return on investment) of your advertising campaign by letting [website owners] assign a monetary value to the activities people complete on [Defendant's] website after clicking [website owners'] ad."[25]

65. Microsoft also utilizes bat.bing.com data for its own purposes, including by using the data to tailor content and target advertisements to users. This profile enables Microsoft to deliver highly targeted ads within Microsoft's extensive advertising network Microsoft's revenue from its advertising network program has exceeded $10 billion as of 2022.[26]

4. Additional Third Party Cookies

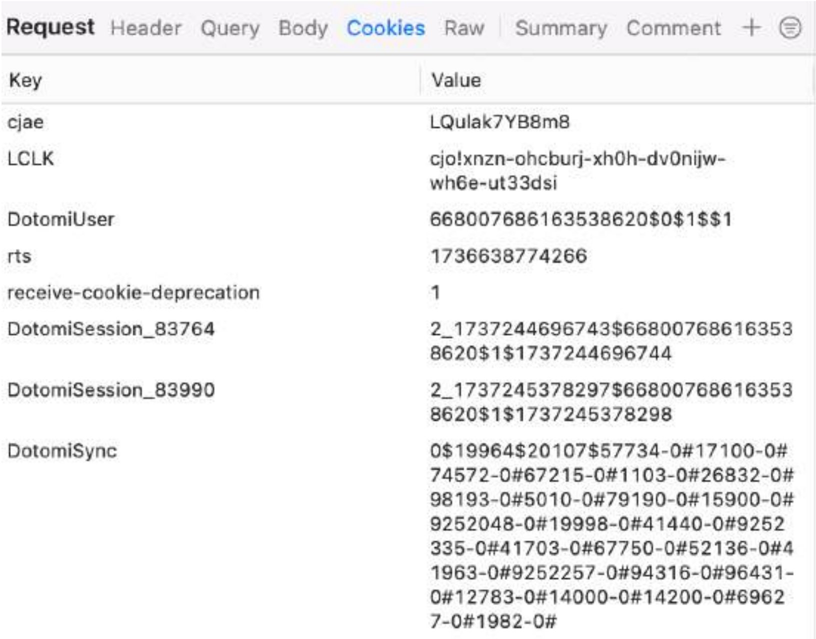
[24] https://help.ads.microsoft.com/#apex/ads/en/60212/0.

[25] https://help.ads.microsoft.com/#apex/ads/en/56680/2.

[26] https://digiday.com/media/microsofts-ad-revenue-hit-10b-and-its-investing-is-a-sleeping-giant-about-to-wake/.

66. Defendant also causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users elect to reject advertising cookies, to and from other domains, including at least dotomi.com, pinterest.com, and blueconic.net.

67. The **dotomi.com** domain is associated with Epsilon Data Management, LLC, a digital marketing company. Dotomi is described as a solution that "provides Personalized Media display advertising that is dynamically adapted in real time at the user and impression level."[27] To ensure that specific users can see advertisements pertaining to them, Epsilon uses various cookies to assign identifiers to them.[28] One such identifier, the "DotomiUser" cookie, is sent to Epsilon when users browse the Websites, even after rejecting cookies:



Key	Value
cjae	LQulak7YB8m8
LCLK	cjo!xnzn-ohcburj-xh0h-dv0nijw-wh6e-ut33dsi
DotomiUser	668007686163538620$0$1$$1
rts	1736638774266
receive-cookie-deprecation	1
DotomiSession_83764	2_1737244696743$668007686163538620$1$1737244696744
DotomiSession_83990	2_1737245378297$668007686163538620$1$1737245378298
DotomiSync	0$19964$20107$57734-0#17100-0#74572-0#67215-0#1103-0#26832-0#98193-0#5010-0#79190-0#15900-0#9252048-0#19998-0#41440-0#9252335-0#41703-0#67750-0#52136-0#41963-0#9252257-0#94316-0#96431-0#12783-0#14000-0#14200-0#69627-0#1982-0#

68. The **pinterest.com** domain is associated with Pinterest, Inc., a popular social media platform that allows users to discover, save, and share ideas as pins in the form of photos and videos. Businesses can upload and showcase their products through "Shop the Look" pins or Product Pins that directly link to e-commerce websites. Businesses install the Pinterest tag on their websites to track ad conversions. As Pinterest explains, "The Pinterest tag is a piece of code

[27] https://www.crunchbase.com/organization/dotomi.

[28] https://legal.epsilon.com/eu/cookie-list.

that you add to your website. It lets Pinterest track visitors to your site, as well as the actions they take on your site after seeing your Pinterest ad. This means you can measure how effective your Pinterest ads are by understanding the actions people take on your website after seeing or engaging with your ad."[29] Pinterest cookies can be used to identify and track people who purchase products, add items to a shopping cart, visit specific pages on the website, and/or search for specific items on the website.[30]

69. The **blueconic.net** domain is associated with BlueConic, Inc., which describes itself as a "customer data operating system … designed to make life easier for the modern front-line marketer."[31] BlueConic's documentation describes how the platform can be used to create and supplement detailed profiles of users, including their contact information, demographics, amount spent, and website visits.[32]

70. These cookies allow these Third Parties to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) demographic information, (v) interests and preferences, (vi) shopping behaviors, (vii) device information, (viii) referring URLs, (ix) session information, (x) user identifiers, and/or (xi) geolocation data.

E. The Private Communications Collected are Valuable.

71. The Private Communications that the Third Parties track and collect by way of the cookies on the Websites are valuable to Defendant as well as the Third Parties. Defendant can use the data to create and analyze the performance of marketing campaigns, website design, product placement, and target specific users or groups of users for advertisements. For instance, if Defendant wanted to market certain of its consumer products, such as holiday specials, to consumers, Defendant could use the data collected by the Third Parties to monitor users who

[29] Pinterest Help Center: Install the Pinterest Tag (available at https://help.pinterest.com/en/business/article/install-the-pinterest-tag).

[30] *See, e.g.*, Pinterest Help Center: Add event codes (available at https://help.pinterest.com/en/business/article/add-event-codes); Pinterest Help Center: View tag parameters and cookies (available at https://help.pinterest.com/en/business/article/pinterest-tag-parameters-and-cookies).

[31] https://www.blueconic.com/.

[32] https://support.blueconic.com/en/articles/247639-blueconic-unified-profiles-glossary.

visit webpages related to specific products, then advertise similar products to those particular users when they visit other webpages. The third-party cookies also enable Defendant to target online advertisements to users when they visit ***other*** websites, even those completely unrelated to Defendant and its products.

72. Data about users' browsing history enables Defendant to spot patterns in users' behavior on the Websites and their interests in, among other things, Defendant's consumer products. On a broader scale, it enables Defendant to gain an understanding of trends happening across its brands and across the consumer retail market. All of this helps Defendant further monetize its Websites and maximize revenue by collecting and analyzing user data.

73. The value of the Private Communications tracked and collected by the Third Parties using cookies on the Websites can be quantified. Legal scholars observe that "[p]ersonal information is an important currency in the new millennium."[33] Indeed, "[t]he monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend." *Id*. "Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information." *Id*.

74. Numerous empirical studies quantify the appropriate value measure for personal data. Generally, the value of personal data is measured as either the consumer's willingness to accept compensation to sell her data or the consumer's willingness to pay to protect her information.

75. Through its false representations and aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties to track users' Private Communications on the Websites using third-party cookies, Defendant is unjustly enriching itself at the cost of consumer privacy and choice, when the consumer could otherwise have the ability to choose if and how they would monetize their data.

PLAINTIFFS' EXPERIENCES

Marco Walsh

[33] *See* Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 Harv. L. Rev. 2055, 2056–57 (2004).

76. In or around December 2024 and January 2025, Plaintiff Walsh visited the Dollar Tree Website to browse information about Dollar Tree's products.

77. When Plaintiff Walsh visited the Dollar Tree Website, it immediately presented him with Defendant's popup cookie consent banner, which provided the option to select the "Reject Advertising Cookies" button. Plaintiff Walsh viewed Defendant's representation on the popup cookie consent banner that, "This website uses cookies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with trusted social media, advertising, and analytics partners." Plaintiff Walsh also viewed Defendant's additional representation that users could "Reject Advertising Cookies."

78. Consistent with his typical practice in rejecting or otherwise declining the placement or use of advertising cookies and tracking technologies, Plaintiff Walsh selected and clicked the "Reject Advertising Cookies" button. Plaintiff Walsh believed that selecting the "Reject Advertising Cookies" button on the popup cookie consent banner found on the Dollar Tree Website would allow him to opt out of, decline, and/or Reject Advertising Cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of tracking data to third-party advertising networks).

79. In selecting the "Reject Advertising Cookies" button Plaintiff Walsh gave Defendant notice that he did not consent to the use or placement of cookies and tracking technologies while browsing the Dollar Tree Website. Further, Plaintiff Walsh specifically rejected, based on Defendant's representations, advertising cookies and those that share information with third party advertising networks. In reliance on these representations and promises, only then did Plaintiff Walsh continue browsing the Dollar Tree Website.

80. Even before the popup cookie consent banner appeared on the screen, Defendant nonetheless caused advertising cookies and tracking technologies, to be placed on Plaintiff Walsh' device and/or transmitted to the Third Parties along with user data, without him knowledge. Accordingly, the popup cookie consent banner's representation to Plaintiff Walsh that he could reject the use and/or placement of advertising cookies and tracking technologies

while he browsed the Dollar Tree Website was false. Contrary to what Defendant made Plaintiff Walsh believe, he did not have a choice about whether third-party cookies would be placed on him device and/or transmitted to the Third Parties along with him user data; rather, Defendant had already caused that to happen.

81. Then, as Plaintiff Walsh continued to browse the Dollar Tree Website in reliance on the promises Defendant made in the cookie consent banner, and despite Plaintiff Walsh' clear rejection of the use and/or placement of such cookies and tracking technologies, Defendant nonetheless continued to cause the placement and/or transmission of such cookies along with user data from the Third Parties on him device. In doing so, Defendant permitted the Third Parties to track and collect Plaintiff Walsh' Private Communications as he browsed the Dollar Tree Website.

82. Defendant's representations that consumers could "Reject Advertising Cookies" while Plaintiff Walsh and users browsed the Dollar Tree Website, were untrue. Had Plaintiff Walsh known this fact, he would not have used the Dollar Tree Website. Moreover, Plaintiff Walsh reviewed the popup cookie consent banner prior to using the Website. Had Defendant disclosed that it would continue to cause advertising cookies and tracking technologies to be stored on consumers' devices even after they choose to Reject Advertising Cookies, Plaintiff Walsh would have noticed it and would not have used the Dollar Tree Website or, at a minimum, he would have interacted with the Website differently.

83. Plaintiff Walsh continues to desire to browse content featured on the Websites. Plaintiff Walsh would like to browse websites that do not misrepresent that users can Reject Advertising Cookies and tracking technologies. If the Websites were programmed to honor users' requests to "Reject Advertising Cookies" and tracking technologies, Plaintiff Walsh would likely browse the Websites again in the future, but will not do so until then. Plaintiff Walsh regularly visits websites that feature content similar to that of the Websites. Because Plaintiff Walsh does not know how the Websites are programmed, which can change over time, and because he does not have the technical knowledge necessary to test whether the Websites

honors users' requests to "Reject Advertising Cookies" and tracking technologies, he will be unable to rely on Defendant's representations when browsing the Websites in the future absent an injunction that prohibits Defendant from making misrepresentations on the Websites. The only way to determine what network traffic is sent to third parties when visiting a website is to use a specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed for use by "developers" (i.e., software developers), whose specialized training enables them to analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff Walsh is not a software developer and has not received training with respect to HTTP network calls.

Howard Yosha

84. In or around October 2024, Plaintiff Yosha visited the Dollar Tree Website to browse information about Dollar Tree's products.

85. When Plaintiff Yosha visited the Dollar Tree Website, it immediately presented him with Defendant's popup cookie consent banner, which provided the option to select the "Reject Advertising Cookies" button. Plaintiff Yosha viewed Defendant's representation on the popup cookie consent banner that, "This website uses cookies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with trusted social media, advertising, and analytics partners." Plaintiff Yosha also viewed Defendant's additional representation that users could "Reject Advertising Cookies."

86. Consistent with his typical practice in rejecting or otherwise declining the placement or use of advertising cookies and tracking technologies, Plaintiff Yosha selected and clicked the "Reject Advertising Cookies" button. Plaintiff Yosha believed that selecting the "Reject Advertising Cookies" button on the popup cookie consent banner found on the Dollar Tree Website would allow him to opt out of, decline, and/or Reject Advertising Cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of tracking data to third-party advertising networks).

87. In selecting the "Reject Advertising Cookies" button Plaintiff Yosha gave Defendant notice that he did not consent to the use or placement of cookies and tracking technologies while browsing the Dollar Tree Website. Further, Plaintiff Yosha specifically rejected, based on Defendant's representations, advertising cookies that share information with third party advertising networks. In reliance on these representations and promises, only then did Plaintiff Yosha continue browsing the Dollar Tree Website.

88. Even before the popup cookie consent banner appeared on the screen, Defendant nonetheless caused advertising cookies and tracking technologies, to be placed on Plaintiff Yosha's device and/or transmitted to the Third Parties along with user data, without his knowledge. Accordingly, the popup cookie consent banner's representation to Plaintiff Yosha that he could reject the use and/or placement of advertising cookies and tracking technologies while he browsed the Dollar Tree Website was false. Contrary to what Defendant made Plaintiff Yosha believe, he did not have a choice about whether third-party cookies would be placed on his device and/or transmitted to the Third Parties along with his user data; rather, Defendant had already caused that to happen.

89. Then, as Plaintiff Yosha continued to browse the Dollar Tree Website in reliance on the promises Defendant made in the cookie consent banner, and despite Plaintiff Yosha's clear rejection of the use and/or placement of such cookies and tracking technologies, Defendant nonetheless continued to cause the placement and/or transmission of such cookies along with user data from the Third Parties on his device. In doing so, Defendant permitted the Third Parties to track and collect Plaintiff Yosha's Private Communications as he browsed the Dollar Tree Website.

90. Defendant's representations that consumers could "Reject Advertising Cookies" while Plaintiff Yosha and users browsed the Dollar Tree Website, were untrue. Had Plaintiff Yosha known this fact, he would not have used the Dollar Tree Website. Moreover, Plaintiff Yosha reviewed the popup cookie consent banner prior to using the Website. Had Defendant disclosed that it would continue to cause advertising cookies and tracking technologies to be

stored on consumers' devices even after they choose to "Reject Advertising Cookies," Plaintiff Yosha would have noticed it and would not have used the Dollar Tree Website or, at a minimum, he would have interacted with the Website differently.

91. Plaintiff Yosha continues to desire to browse content featured on the Websites. Plaintiff Yosha would like to browse websites that do not misrepresent that users can "Reject Advertising Cookies" and tracking technologies. If the Websites were programmed to honor users' requests to "Reject Advertising Cookies" and tracking technologies, Plaintiff Yosha would likely browse the Websites again in the future, but will not do so until then. Plaintiff Yosha regularly visits websites that feature content similar to that of the Websites. Because Plaintiff Yosha does not know how the Websites are programmed, which can change over time, and because he does not have the technical knowledge necessary to test whether the Websites honors users' requests to "Reject Advertising Cookies" and tracking technologies, he will be unable to rely on Defendant's representations when browsing the Websites in the future absent an injunction that prohibits Defendant from making misrepresentations on the Websites. The only way to determine what network traffic is sent to third parties when visiting a website is to use a specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed for use by "developers" (i.e., software developers), whose specialized training enables them to analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff Yosha is not a software developer and has not received training with respect to HTTP network calls.

Erica Maldonado

92. In or around October 2024, Plaintiff Maldonado visited the Dollar Tree Website to browse information about Dollar Tree's products.

93. When Plaintiff Maldonado visited the Dollar Tree Website, it immediately presented her with Defendant's popup cookie consent banner, which provided the option to select the "Reject Advertising Cookies" button. Plaintiff Maldonado viewed Defendant's representation on the popup cookie consent banner that, "This website uses cookies to enhance

user experience and to analyze performance and traffic on our website. We also share information about your use of our site with trusted social media, advertising, and analytics partners." Plaintiff Maldonado also viewed Defendant's additional representation that users could "Reject Advertising Cookies."

94. Consistent with her typical practice in rejecting or otherwise declining the placement or use of advertising cookies and tracking technologies, Plaintiff Maldonado selected and clicked the "Reject Advertising Cookies" button. Plaintiff Maldonado believed that selecting the "Reject Advertising Cookies" button on the popup cookie consent banner found on the Dollar Tree Website would allow her to opt out of, decline, and/or Reject Advertising Cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of tracking data to third-party advertising networks).

95. In selecting the "Reject Advertising Cookies" button Plaintiff Maldonado gave Defendant notice that she did not consent to the use or placement of cookies and tracking technologies while browsing the Dollar Tree Website. Further, Plaintiff Maldonado specifically rejected, based on Defendant's representations, advertising cookies that share information with third party advertising networks. In reliance on these representations and promises, only then did Plaintiff Maldonado continue browsing the Dollar Tree Website.

96. Even before the popup cookie consent banner appeared on the screen, Defendant nonetheless caused advertising cookies and tracking technologies, to be placed on Plaintiff Maldonado's device and/or transmitted to the Third Parties along with user data, without her knowledge. Accordingly, the popup cookie consent banner's representation to Plaintiff Maldonado that she could reject the use and/or placement of advertising cookies and tracking technologies while she browsed the Dollar Tree Website was false. Contrary to what Defendant made Plaintiff Maldonado believe, she did not have a choice about whether third-party cookies would be placed on her device and/or transmitted to the Third Parties along with her user data; rather, Defendant had already caused that to happen.

97. Then, as Plaintiff Maldonado continued to browse the Dollar Tree Website in reliance on the promises Defendant made in the cookie consent banner, and despite Plaintiff Maldonado's clear rejection of the use and/or placement of such cookies and tracking technologies, Defendant nonetheless continued to cause the placement and/or transmission of such cookies along with user data from the Third Parties on her device. In doing so, Defendant permitted the Third Parties to track and collect Plaintiff Maldonado's Private Communications as she browsed the Dollar Tree Website.

98. Defendant's representations that consumers could "Reject Advertising Cookies" while Plaintiff Maldonado and users browsed the Dollar Tree Website, were untrue. Had Plaintiff Maldonado known this fact, she would not have used the Dollar Tree Website. Moreover, Plaintiff Maldonado reviewed the popup cookie consent banner prior to using the Website. Had Defendant disclosed that it would continue to cause advertising cookies and tracking technologies to be stored on consumers' devices even after they choose to "Reject Advertising Cookies," Plaintiff Maldonado would have noticed it and would not have used the Dollar Tree Website or, at a minimum, she would have interacted with the Website differently.

99. Plaintiff Maldonado continues to desire to browse content featured on the Websites. Plaintiff Maldonado would like to browse websites that do not misrepresent that users can "Reject Advertising Cookies" and tracking technologies. If the Websites were programmed to honor users' requests to "Reject Advertising Cookies" and tracking technologies, Plaintiff Maldonado would likely browse the Websites again in the future, but will not do so until then. Plaintiff Maldonado regularly visits websites that feature content similar to that of the Websites. Because Plaintiff Maldonado does not know how the Websites are programmed, which can change over time, and because she does not have the technical knowledge necessary to test whether the Websites honors users' requests to "Reject Advertising Cookies" and tracking technologies, she will be unable to rely on Defendant's representations when browsing the Websites in the future absent an injunction that prohibits Defendant from making misrepresentations on the Websites. The only way to determine what network traffic is sent to

third parties when visiting a website is to use a specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed for use by "developers" (i.e., software developers), whose specialized training enables them to analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff Maldonado is not a software developer and has not received training with respect to HTTP network calls.

CLASS ALLEGATIONS

100. Plaintiffs bring this Class Action Complaint on behalf of themselves and a proposed class of similarly situated persons, pursuant to Rules 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure. Plaintiffs seek to represent the following group of similarly situated persons, defined as follows:

> **Class**: All persons who browsed either of the Websites in the State of California after clicking the "Reject Advertising Cookies" button in the popup cookies consent banner within the four years preceding the filing of this Complaint (the "Class Period").

101. This action has been brought and may properly be maintained as a class action against Defendant because there is a well-defined community of interest in the litigation and the proposed class is easily ascertainable.

102. **Numerosity:** Plaintiffs do not know the exact size of the Class, but they estimate that it is composed of more than 100 persons. The persons in the Class are so numerous that the joinder of all such persons is impracticable and the disposition of their claims in a class action rather than in individual actions will benefit the parties and the courts.

103. **Common Questions Predominate:** This action involves common questions of law and fact to the Class because each class member's claim derives from the same unlawful conduct that led them to believe that Defendant would not cause third-party cookies to be placed on their browsers and devices and/or transmitted to third parties along with user data, after Class members chose to "Reject Advertising Cookies" and tracking technologies on the Websites, nor

would Defendant permit third parties to track and collect Class members' Private Communications as Class members browsed the Websites.

104. The common questions of law and fact predominate over individual questions, as proof of a common or single set of facts will establish the right of each member of the Class to recover. The questions of law and fact common to the Class include:

a. Whether Defendant's actions violate California laws invoked herein; and

b. Whether Plaintiffs and Class members are entitled to damages, restitution, injunctive and other equitable relief, reasonable attorneys' fees, prejudgment interest and costs of this suit.

105. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, Plaintiffs, like the other Class members, visited the Websites, rejected advertising cookies, and had their confidential Private Communications intercepted by the Third Parties.

106. **Adequacy of Representation:** Plaintiffs will fairly and adequately protect the interests of all Class members because it is in their best interests to prosecute the claims alleged herein to obtain full compensation due to them for the unfair and illegal conduct of which they complain. Plaintiffs also have no interests in conflict with, or antagonistic to, the interests of Class members. Plaintiffs have retained highly competent and experienced class action attorneys to represent their interests and those of the Class. By prevailing on their claims, Plaintiffs will establish Defendant's liability to all Class members. Plaintiffs and their counsel have the necessary financial resources to adequately and vigorously litigate this class action, and Plaintiffs and counsel are aware of their fiduciary responsibilities to the Class members and are determined to diligently discharge those duties by vigorously seeking the maximum possible recovery for Class members.

107. **Superiority:** There is no plain, speedy, or adequate remedy other than by maintenance of this class action. The prosecution of individual remedies by members of the Class

will tend to establish inconsistent standards of conduct for Defendant and result in the impairment of Class members' rights and the disposition of their interests through actions to which they were not parties. Class action treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would engender. Furthermore, as the damages suffered by each individual member of the Class may be relatively small, the expenses and burden of individual litigation would make it difficult or impossible for individual members of the class to redress the wrongs done to them, while an important public interest will be served by addressing the matter as a class action. Plaintiffs are unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

First Cause of Action: Invasion of Privacy

108. Plaintiffs reallege and incorporate the paragraphs of this Complaint as if set forth herein.

109. To plead an invasion of privacy claim, Plaintiffs must show an invasion of (i) a legally protected privacy interest; (ii) where Plaintiffs had a reasonable expectation of privacy in the circumstances; and (iii) conduct by Defendant constituting a serious invasion of privacy.

110. Defendant has intruded upon the following legally protected privacy interests of Plaintiffs and Class members: (i) the California Invasion of Privacy Act, as alleged herein; (ii) the California Constitution, which guarantees Californians the right to privacy; (iii) the California Wiretap Acts as alleged herein; (iv) Cal. Penal Code § 484(a), which prohibits the knowing theft or defrauding of property "by any false or fraudulent representation or pretense;" and (v) Plaintiffs' and Class members' Fourth Amendment right to privacy.

111. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances, as Defendant affirmatively promised users they could "Reject Advertising

Cookies" and tracking technologies before proceeding to browse the Websites. Plaintiffs and other Class members directed their electronic devices to access the Websites and, when presented with the popup cookies consent banner on the Websites, Plaintiffs and Class members rejected advertising cookies and reasonably expected that their and their rejection of advertising cookies and tracking technologies would be honored. That is, they reasonably believed that Defendant would not permit the Third Parties to store and send advertising cookies and/or use other such tracking technologies on their devices while they browsed the Websites. Plaintiffs and Class members also reasonably expected that, if they rejected such cookies and/or tracking technologies, Defendant would not permit the Third Parties to track and collect Plaintiffs' and Class members' Private Communications, including their browsing history, visit history, Website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, on the Websites.

112. Such information is "personal information" under California law, which defines personal information as including "Internet or other electronic network activity information," such as "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

113. Defendant, in violation of Plaintiffs' and other Class members' reasonable expectation of privacy and without their consent, permits the Third Parties to use cookies and other tracking technologies to collect, track, and compile users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data. The data that Defendant allowed third parties to collect enables the Third Parties to, *inter alia*, create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics; create audience segments based on shared traits (such as millennials, tech enthusiasts, etc.); and perform targeted advertising and marketing analytics. Further, the Third Parties share user data

and/or the user profiles to unknown parties to further their financial gain. The consumer profiles are and can be used to further invade Plaintiffs' and users' privacy, by allowing third parties to learn intimate details of their lives, and target them for advertising and other purposes, as described herein, thereby harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them.

114. Defendant's actions constituted a serious invasion of privacy in that it invaded a zone of privacy protected by the Fourth Amendment (i.e., one's personal communications), and violated criminal laws on wiretapping and invasion of privacy. These acts constitute an egregious breach of social norms that is highly offensive.

115. Defendant's intrusion into Plaintiffs' privacy was also highly offensive to a reasonable person.

116. Defendant lacked a legitimate business interest in causing the placement and/or transmission of third-party cookies along with user data that allowed the Third Parties to track, intercept, receive, and collect Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, without their consent.

117. Plaintiffs and Class members have been damaged by Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

118. Plaintiffs and Class members seeks appropriate relief for that injury, including but not limited to, damages that will compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiffs' and Class members' privacy.

119. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and

Plaintiffs' and Class members' rejection of the Websites' use of advertising cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Second Cause of Action: Intrusion Upon Seclusion

120. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

121. To assert a claim for intrusion upon seclusion, Plaintiffs must plead (i) that Defendant intentionally intruded into a place, conversation, or matter as to which Plaintiffs had a reasonable expectation of privacy; and (ii) that the intrusion was highly offensive to a reasonable person.

122. By permitting third-party cookies to be stored on consumers' devices without consent, which enabled the Third Parties to track and collect Plaintiffs' and Class members' Private Communications, including their browsing history, visit history, Website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, in violation of Defendant's representations otherwise in the popup cookie consent banner, Defendant intentionally intruded upon the solitude or seclusion of Website users. Defendant effectively placed the Third Parties in the middle of communications to which they were not invited, welcomed, or authorized.

123. The Third Parties' tracking and collecting of Plaintiffs' and Class member's Private Communications on the Websites using third-party cookies that Defendant caused to be stored on users' devices—and to be transmitted to Third Parties—was not authorized by Plaintiffs and Class members, and, in fact, those Website users specifically chose to "Reject Advertising Cookies."

124. Plaintiffs and the Class members had an objectively reasonable expectation of privacy surrounding their Private Communications on the Websites based on Defendant's promise that users could "Reject Advertising Cookies", as well as state criminal and civil laws designed to protect individual privacy.

125. Defendant's intentional intrusion into Plaintiffs' and other users' Private Communications would be highly offensive to a reasonable person given that Defendant represented that Website users could "Reject Advertising Cookies" when, in fact, Defendant caused such third-party cookies to be stored on consumers' devices and browsers, and to be transmitted to third parties, even when consumers rejected all such cookies. Indeed, Plaintiffs and Class members reasonably expected, based on Defendant's false representations, that when they rejected advertising cookies and tracking technologies, Defendant would not cause such third-party cookies to be stored on their devices or permit the Third Parties to obtain their Private Communications on the Websites, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

126. Defendant's conduct was intentional and intruded on Plaintiffs' and users' Private Communications on the Websites.

127. Plaintiffs and Class members have been damaged by Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

128. Plaintiffs and Class members seeks appropriate relief for that injury, including but not limited to, damages that will compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiffs' and Class members' privacy.

129. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and Plaintiffs' and Class members' rejection of the Websites' use of advertising cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy Act (California Penal Code § 631)

130. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

131. California Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars . . . .

132. The California Supreme Court has repeatedly stated an "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line permits an outsider to tap his telephone or listen in on the call." *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added).

133. Further, as the California Supreme Court has held, in explaining the legislative purpose behind CIPA:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and *its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.*
>
> As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication— the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas, 38 Cal. 3d at 360-61 (emphasis supplied; internal citations omitted).

134. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under § 631(a), Plaintiffs need only establish that Defendant, "by means of any machine, instrument, contrivance, or in any other manner," did ***any*** of the following:

> [i] Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;
>
> [ii] Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any

> message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;
>
> [iii] Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained

Cal. Penal Code § 631(a).

135. CIPA § 631(a) also penalizes those who [iv] "aid[], agree[] with, employ[], or conspire[] with any person" who conducts the aforementioned wiretapping, or those who "permit" the wiretapping.

136. Defendant is a "person" within the meaning of California Penal Code § 631.

137. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *see also Bradley v. Google, Inc.*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications.").

138. The Third Parties' cookies—as well as the software code of the Third Parties responsible for placing the cookies and transmitting data from user devices to the Third Parties—constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA (and, even if they do not, Defendant's deliberate and purposeful scheme that facilitated the interceptions falls under the broad statutory catch-all category of "any other manner").

139. Each of the Third Parties is a "separate legal entity that offers [a] 'software-as-a-service' and not merely a passive device." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, the Third Parties had the capability to use the wiretapped information for their own purposes and, as alleged above, they did in fact use the wiretapped information for their own business purposes. Accordingly, the Third Parties were third parties to any communication between Plaintiffs and Class members, on the one hand, and Defendant, on the

other. *Id.* at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

140. Under § 631(a), Defendant must show it had the consent of all parties to a communication.

141. At all relevant times, the Websites caused Plaintiffs and Class members' browsers to store the Third Parties' cookies and to transmit those cookies alongside Private Communications—including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data—to the Third Parties without Plaintiffs' and Class members' consent. By configuring the Websites in this manner, Defendant willfully aided, agreed with, employed, permitted, or otherwise enabled the Third Parties to wiretap Plaintiffs and Class members using the Third Parties' cookies and to accomplish the wrongful conduct alleged herein.

142. At all relevant times, by their cookies and corresponding software code, the Third Parties willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, attempted to read, and/or learned the contents or meaning of electronic communications of Plaintiffs and Class members, on the one hand, and Defendant, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

143. The Private Communications of Plaintiffs and Class members, on the one hand, and Defendant, on the other, that the Third Parties automatically intercepted directly communicates the Website user's affirmative decisions, actions, choices, preferences, and activities, which constitute the "contents" of electronic communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

144. At all relevant times, the Third Parties used or attempted to use the Private Communications automatically intercepted by their cookie tracking technologies for their own purposes.

145. Plaintiffs and Class members did not provide their prior consent to the Third Parties' intentional access, interception, reading, learning, recording, collection, and usage of Plaintiffs' and Class members' electronic communications. Nor did Plaintiffs and Class members provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties' conduct. On the contrary, Plaintiffs and Class members expressly declined to allow third-party advertising cookies and tracking technologies to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic communications by choosing to reject advertising cookies in the consent banner.

146. The wiretapping of Plaintiffs and Class members occurred in California, where Plaintiffs and Class members accessed the Websites and where the Third Parties—as enabled by Defendant—routed Plaintiffs' and Class members' electronic communications to Third Parties' servers. Among other things, the cookies, as well as the software code responsible for placing the cookies and transmitting them and other Private Communications to the Third Parties, resided on Plaintiffs' California-located device. In particular, the user's California-based device, after downloading the software code from the Third Parties' servers, (i) stored the code onto the user's disk; (ii) converted the code into machine-executable format; and (iii) executed the code, causing the transmission of data (including cookie data) to and from the Third Parties.

147. Plaintiffs and Class members have suffered loss by reason of these violations, including, but not limited to, (i) violation of their right to privacy, (ii) loss of value their Private Communications, (iii) damage to and loss of Plaintiffs' and Class members' property right to control the dissemination and use of their Private Communications, and (iv) loss of their Private Communications to the Third Parties with no consent.

148. Pursuant to California Penal Code § 637.2, Plaintiffs and Class members have been injured by the violations of California Penal Code § 631, and each seeks statutory damages

of the greater of $5,000, or three times the amount of actual damages, for each of Defendant's violations of CIPA § 631(a), as well as injunctive relief.

149. Unless enjoined, Defendant will continue to commit the illegal acts alleged herein including, but not limited to, permitting third parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant. Plaintiffs, Class members, and the general public continue to be at risk because Plaintiffs, Class members, and the general public frequently use the internet to search for information and content related to consumer retail products. Plaintiffs, Class members, and the general public continue to desire to use the internet for that purpose. Plaintiffs, Class members, and the general public have no practical way to know if their request to reject advertising cookies and tracking technologies will be honored and/or whether Defendant will permit third parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant. Further, Defendant has already permitted the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant and will continue to do so unless and until enjoined.

<u>Fourth Cause of Action</u>: Use of a Pen Register in Violation of the California Invasion of Privacy Act (California Penal Code § 638.51)

150. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

151. The California Invasion of Privacy Act, codified at Cal. Penal Code §§ 630 to 638, includes the following statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

152. California Penal Code Section 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

153. A “pen register” is a “a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication.” Cal. Penal Code § 638.50(b).

154. The Third Parties’ cookies and the corresponding software code installed by Defendant on its Websites are each “pen registers” because they are “device[s] or process[es]” that “capture[d]” the “routing, addressing, or signaling information”—including, the IP address and user-agent information—from the electronic communications transmitted by Plaintiffs’ and the Class’s computers or devices. Cal. Penal Code § 638.50(b).

155. At all relevant times, Defendant caused the Third Parties’ cookies and the corresponding software code—which are pen registers—to be placed on Plaintiffs’ and Class members’ browsers and devices, and/or to be used to transmit Plaintiffs’ and Class members’ IP address and user-agent information. *See Greenley v. Kochava,* 2023 WL 4833466, at *15-16 (S.D. Cal. July 27, 2023); *Shah v. Fandom, Inc.*, 2024 U.S. Dist. LEXIS 193032, at *5-11 (N.D. Cal. Oct. 21, 2024).

156. Some of the information collected by the Third Parties’ cookies and the corresponding software, including IP addresses and user-agent information, does not constitute the content of Plaintiffs’ and the Class members’ electronic communications with the Websites. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1008 (9th Cir. 2014). (“IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication…”) (cleaned up).

157. Plaintiffs and Class members did not provide their prior consent to Defendant’s use of third-party cookies and the corresponding software. On the contrary, Plaintiffs and the Class members informed Defendant that they did not consent to the Websites’ use of third-party cookies by clicking the “Reject Advertising Cookies” button in the cookie consent banner.

158. Defendant did not obtain a court order to install or use the third-party cookies and corresponding software to track and collect Plaintiffs' and Class member's IP addresses and user-agent information.

159. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members suffered losses and were damaged in an amount to be determined at trial.

160. Pursuant to Penal Code § 637.2(a)(1), Plaintiffs and Class members are also entitled to statutory damages of $5,000 for each of Defendant's violations of § 638.51(a).

Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation

161. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

162. Defendant fraudulently and deceptively informed Plaintiffs and Class members that they could "Reject Advertising Cookies."

163. However, despite Defendant's representations otherwise, Defendant caused third-party cookies and software code to be stored on consumers' devices, and to be transmitted to the Third Parties alongside Private Communications, even after users clicked the "Reject Advertising Cookies" button in the popup cookie consent banner. These cookies and corresponding software code allowed the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' Private Communications, even when consumers had previously chosen to "Reject Advertising Cookies."

164. These misrepresentations and omissions were known exclusively to, and actively concealed by Defendant, not reasonably known to Plaintiffs and Class members, and material at the time they were made. Defendant knew, or should have known, how the Websites functioned, including the Third Party's resources it installed on the Websites and the third-party cookies in use on the Websites, through testing the Websites, evaluating its performance metrics by means of its accounts with the Third Parties, or otherwise, and knew, or should have known, that the Websites' programming allowed the third-party cookies to be placed on users'—including Plaintiffs'—browsers and devices and/or transmitted to the Third Parties along with users' Private Communications even after users attempted to "Reject Advertising Cookies", which

Defendant promised its users they could do. Defendant’s misrepresentations and omissions concerned material facts that were essential to the analysis undertaken by Plaintiffs and Class members as to whether to use the Websites. In misleading Plaintiffs and Class members and not so informing them, Defendant breached its duty to Plaintiffs and Class members. Defendant also gained financially from, and as a result of, its breach.

165. Plaintiffs and Class members relied to their detriment on Defendant’s misrepresentations and fraudulent omissions.

166. Plaintiffs and Class members have suffered an injury-in-fact, including the loss of money and/or property, as a result of Defendant’s unfair, deceptive, and/or unlawful practices, including the unauthorized interception of their Private Communications, including their browsing history, visit history, Website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, which have value as demonstrated by the use and sale of consumers’ browsing activity, as alleged above. Plaintiffs and Class members have also suffered harm in the form of diminution of the value of their private and personally identifiable information and communications.

167. Defendant’s actions caused damage to and loss of Plaintiffs’ and Class members’ property right to control the dissemination and use of their personal information and communications.

168. Defendant’s representation that consumers could reject advertising cookies if they clicked the “Reject Advertising Cookies” button was untrue. Again, had Plaintiffs and Class members known these facts, they would not have used the Websites. Moreover, Plaintiffs and Class members reviewed the popup cookie consent banner prior to their interactions with the Websites. Had Defendant disclosed that it caused third-party advertising cookies to be stored on Website visitors’ devices that share information with third parties even after they choose to “Reject Advertising Cookies,” Plaintiffs and Class members would have noticed it and would not have interacted with the Websites.

169. By and through such fraud, deceit, misrepresentations and/or omissions, Defendant intended to induce Plaintiffs and Class members to alter their positions to their detriment. Specifically, Defendant fraudulently and deceptively induced Plaintiffs and Class members to, without limitation, use the Websites under the mistaken belief that Defendant would not permit third parties to obtain users' Private Communications when consumers chose to reject advertising cookies. As a result, Plaintiffs and the Class provided more personal data than they would have otherwise.

170. Plaintiffs and Class members justifiably and reasonably relied on Defendant's misrepresentations and omissions, and, accordingly, were damaged by Defendant's conduct.

171. As a direct and proximate result of Defendant's misrepresentations and/or omissions, Plaintiffs and Class members have suffered damages, as alleged above, and are entitled to just compensation, including monetary damages.

172. Plaintiffs and Class members seek punitive damages because Defendant's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and Class members and made in conscious disregard of Plaintiffs' and Class members' rights and Plaintiffs' and Class members' rejection of the Websites' use of advertising cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Sixth Cause of Action: Unjust Enrichment

173. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

174. Defendant created and implemented a scheme to increase its own profits through a pervasive pattern of false statements and fraudulent omissions.

175. Defendant was unjustly enriched as a result of its wrongful conduct, including through its misrepresentation that users could "Reject Advertising Cookies" and by permitting the Third Parties to store and transmit cookies on Plaintiffs' and Class members' devices and browsers, which permitted the Third Parties to track and collect users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs,

session information, user identifiers, and/or geolocation data, even after Class members rejected such cookies.

176. Plaintiffs and Class members' Private Communications have conferred an economic benefit on Defendant.

177. Defendant has been unjustly enriched at the expense of Plaintiffs and Class members, and Defendant has unjustly retained the benefits of its unlawful and wrongful conduct.

178. Defendant appreciated, recognized, and chose to accept the monetary benefits that Plaintiffs and Class members conferred onto Defendant at their detriment. These benefits were the expected result of Defendant acting in its pecuniary interest at the expense of Plaintiffs and Class members.

179. It would be unjust for Defendant to retain the value of Plaintiffs' and Class members' property and any profits earned thereon.

180. There is no justification for Defendant's enrichment. It would be inequitable, unconscionable, and unjust for Defendant to be permitted to retain these benefits because the benefits were procured as a result of its wrongful conduct.

181. Plaintiffs and Class members are entitled to restitution of the benefits Defendant unjustly retained and/or any amounts necessary to return Plaintiffs and Class members to the position they occupied prior to having their Private Communications tracked and collected by the Third Parties.

182. Plaintiffs pleads this claim separately, as well as in the alternative, to other claims, as without such claims Plaintiffs would have no adequate legal remedy.

Seventh Cause of Action: Breach of Contract

183. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

184. Defendant's relationship with its users is governed by the Website's Privacy Policy, which explains:

> We at Dollar Tree, Inc., Dollar Tree Stores, Inc., Family Dollar Stores, Inc., and their affiliates ("Dollar Tree," "We," "Us," or "Our") care deeply about privacy, security, and online safety. This Privacy Policy ("Policy") is designed to inform you about how we collect, use, safeguard, and disclose your "Personal Information" (as defined

> below), and our commitment to using the Personal Information we collect in a transparent and respectful manner. This Policy also tells you about your rights and choices with respect to your Personal Information, and how you can reach us to get answers to your questions.

185. The Website's Privacy Policy contains enforceable promises that Defendant made to Plaintiffs and Class members, including, but not limited to, the following provision:

> In addition, depending on your location and applicable laws, we may give you the option of adjusting your preferences regarding the categories of Cookies we use. When this option is available, you can configure your personal settings on our 'Manage Cookies' or via other options that may be available on the relevant Service.

186. Defendant breached these duties and violated these promises by causing third-party cookies to be stored on consumers' devices and browsers that enabled the Third Parties to track and collect Plaintiffs' and Class member's Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even though Defendant represented that Plaintiffs and other users could "Reject Advertising Cookies." Plaintiffs and Class members, in fact, chose to reject such cookies by selecting the "Reject Advertising Cookies" button.

187. At all relevant times and in all relevant ways, Plaintiffs and Class members performed their obligations under the Privacy Policy or were excused from performance of such obligations through the unknown and unforeseen conduct of others.

188. Defendant's conduct in permitting the Third Parties to track and collect the Private Communications of Website users who chose to reject advertising cookies and tracking technologies evaded the spirit of the bargain made between Defendant and Plaintiffs and Class members since it caused Plaintiffs and Class members to surrender more data than they had otherwise bargained for.

189. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and Class members did not receive the full benefit of the bargain, and instead received services from Defendant that were less valuable than described in the Privacy Policy. Plaintiffs and Class

members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendant's partial, deficient, and/or defective performance.

190. As a direct consequence of the breaches of contract and violations of promises described above, Plaintiffs and Class members seek nominal damages, general damages, compensatory damages, consequential damages, unjust enrichment, and any other just relief.

Eighth Cause of Action: Breach of Implied Covenant of Good Faith and Fair Dealing

191. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

192. Defendant's relationship with its users is governed by the Website's Privacy Policy, which explains:

> We at Dollar Tree, Inc., Dollar Tree Stores, Inc., Family Dollar Stores, Inc., and their affiliates ("Dollar Tree," "We," "Us," or "Our") care deeply about privacy, security, and online safety. This Privacy Policy ("Policy") is designed to inform you about how we collect, use, safeguard, and disclose your "Personal Information" (as defined below), and our commitment to using the Personal Information we collect in a transparent and respectful manner. This Policy also tells you about your rights and choices with respect to your Personal Information, and how you can reach us to get answers to your questions.

193. The Website's Privacy Policy contains enforceable promises that Defendant made to Plaintiffs and Class members, including, but not limited to, the following provision:

> In addition, depending on your location and applicable laws, we may give you the option of adjusting your preferences regarding the categories of Cookies we use. When this option is available, you can configure your personal settings on our 'Manage Cookies' or via other options that may be available on the relevant Service.

194. Defendant breached these duties and violated these promises by causing third-party cookies to be stored on consumers' devices and browsers that enabled the Third Parties to track and collect Plaintiffs' and Class member's Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even though Defendant represented that Plaintiffs and other users could reject advertising cookies. Plaintiffs and Class members, in fact,

chose to reject such cookies by selecting the "Reject Advertising Cookies" button. California law recognizes the implied covenant of good faith and fair dealing in every contract.

195. In dealing between Defendant and its Website users, Defendant is invested with discretionary power affecting the rights of its users.

196. Defendant purports to respect and protect its Website users' privacy.

197. Despite their contractual promises to allow consumers to reject advertising cookies and other tracking technologies, Defendant took actions outside that contractual promise to deprive consumers, including Plaintiffs and other users similarly situated, of benefits of their contracts with Defendant.

198. Defendant's allowance of third parties to track and collect Website users' Private Communications with Defendant was objectively unreasonable given its privacy promises.

199. Defendant's conduct in permitting third parties to track and collect the Private Communications of Website users who chose to reject advertising cookies and tracking technologies evaded the spirit of the bargain made between Defendant and Plaintiffs and Class members since it caused Plaintiffs and Class members to surrender more data than they had otherwise bargained for.

200. As a result of Defendant's misconduct and breach of its duty of good faith and fair dealing, Plaintiffs and Class members suffered damages. Plaintiffs and Class members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of providing their personal information, which, as alleged above, has ascertainable value.

201. As a direct consequence of the breach of the implied covenant of good faith and fair dealing described above, Plaintiffs and Class members seek nominal damages, general damages, compensatory damages, consequential damages, and any other just relief.

Ninth Cause of Action: Trespass to Chattels

202. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

203. Defendant, intentionally and without consent or other legal justification, caused cookies to be stored on Plaintiffs' and Class members' browsers and devices, which enabled the Third Parties and Defendant to track and collect Plaintiffs' and Class members' Private Communications and use the data collected for their own advantage, as described above.

204. Defendant was unjustly enriched as a result of its wrongful conduct, including through its misrepresentation that users could "Reject Advertising Cookies" and tracking technologies, and through their failure to disclose that Defendant causes third-party cookies to be stored on consumers' devices and browsers, which cause the Third Parties and Defendant to track and collect Plaintiffs' and Class members' Private Communications even after consumers chose to reject such cookies.

205. Defendant intentionally caused third party software code to be stored onto Plaintiffs' and Class members' devices, knowing that the code would be executed by those devices. The software code then placed and/or transmitted cookies along with Plaintiffs' and Class members' Private Communications to the Third Parties. These intentional acts interfered with Plaintiffs' and Class members' use of the following personal property owned, leased, or controlled by Plaintiffs and other users: (a) their computers and other electronic devices; and (b) their personally identifiable information.

206. Defendant's trespass of Plaintiffs' and other users' computing devices resulted in harm to Plaintiffs and other users and caused Plaintiffs and other users the following damages:

a. Nominal damages for trespass;

b. Reduction of storage, disk space, and performance of Plaintiffs' and other users' computing devices; and

c. Loss of value of Plaintiffs' and other users' computing devices.

PRAYER FOR RELIEF

WHEREFORE, reserving all rights, Plaintiffs, on behalf of themselves and the Class members, respectfully requests judgment against Defendant as follows:

A. Certification of the proposed Class, including appointment of Plaintiffs' counsel as class counsel;

B. An award of compensatory damages, including statutory damages where available, to Plaintiffs and Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, including both pre- and post-judgment interest thereon;

C. An award of punitive damages;

D. An award of nominal damages;

E. An order for full restitution;

F. An order requiring Defendant to disgorge revenues and profits wrongfully obtained;

G. An order temporarily and permanently enjoining Defendant from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

H. For reasonable attorneys' fees and the costs of suit incurred; and

I. For such further relief as may be just and proper.

Dated: February 14, 2025

GUTRIDE SAFIER LLP

/s/Seth A. Safier/s/

Seth A. Safier (State Bar No. 197427)
seth@gutridesafier.com
Marie A. McCrary (State Bar No. 262670)
marie@gutridesafier.com
Todd Kennedy (State Bar No. 250267)
todd@gutridesafier.com
Kali R. Backer (State Bar No. 342492)
kali@gutridesafier.com
100 Pine Street, Suite 1250
San Francisco, CA 94111
Telephone: (415) 639-9090
Facsimile: (415) 449-6469

Attorneys for Plaintiffs